MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

SUMMER – 2023 EXAMINATION MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills).
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate"s answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate"s understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

Q. No.	Sub Q.N.	Answer	Marking Scheme

1.		**Attempt any FIVE of the following:**	**10**
	(a) **Ans.**	**Draw and label sketch if IPv4 packet format.**	**2M** *2M Diagram*
	(b) **Ans.**	**List any two extension headers of IPv6 protocol.**	**2M**

Version(4 bits)	Header length (4 bits)	Type of service (8 bits)	Total length (16 bits)	
Identification (16 bits)			Flags (3 bits)	Fragment offset (13 bits)
Time to live (8 bits)		Protocol (8 bits)	Header checksum (16 bits)	
Source address (32 bits)				
Destination address (32 bits)				
Options and padding (if any)				

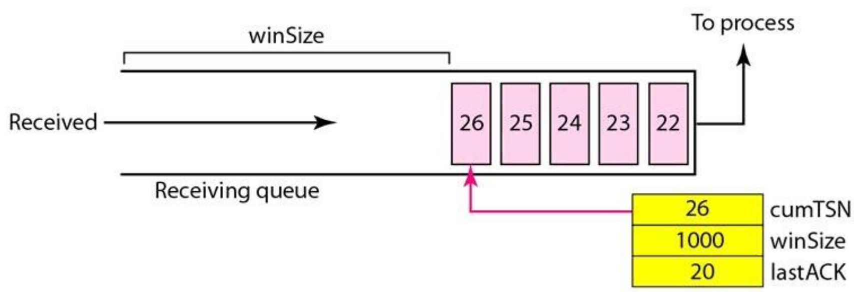
		1. Hop by Hop option 2. Source routing 3. Fragmentation 4. Authentication 5. Encrypted security payload 6. Destination option	*Any two*
	(c) Ans.	**Define Inter Domain routing.** Routing between autonomous system is referred to as interdomain routing.	**2M** ***Correct definition***
	(d) Ans.	**State the use of 6 flags in TCP header.** There are 6, 1-bit control bits that control connection establishment, termination, abortion, flow control etc.. 1. URG: The urgent pointer is valid if it is 1. 2. ACK: ACK bit is set to 1 to indicate the acknowledgement member is valid. 3. PSH: The receiver should pass this data to application as soon as possible. 4. RST: This flag is used to reset connection. 5. SYN: Synchronize sequence number to initiate a connection. 6. FIN: It is used to release connection	**2M** ***Correct use 2M***

	(e) **Ans**	**Differentiate between FTP and TFTP (any two points)**	**2M**

FTP	TFTP
File Transfer Protocol	Trivial File Transfer Protocol
It uses two connections	It uses one connection
Provides many commands	Provides only 5 commands
Uses TCP	Uses UDP
Client must login to server	No Login procedure
Allow for user authentication	Doesn't allow user authentication
It is reliable	It is unreliable

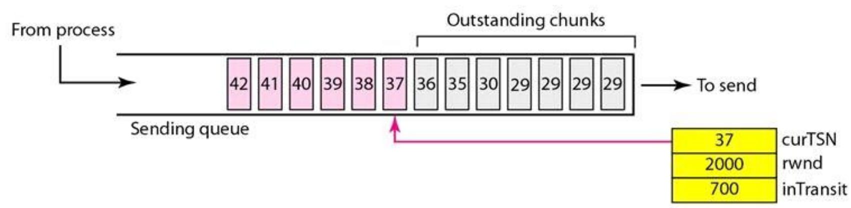
1m each point

	(f) **Ans.**	**List types of ICMPv4 messages.** **ICMP Messages are of two types:-** 1. Error reporting messages: If a host or router encounter a problem after processing an IP problem, then it was a error reporting message for reporting the problem. 2. Query Messages: A host or a network manager can used the query messages to get some specific information from a router to another host.	**2M** ***Any two advantages 1M each***
	(g) **Ans.**	**State the importance of IPv6 over IPv4.** i) huge number of IP addresses: IPv6 has 128-bit addresses when compared to 32-bit addresses of IPv4 which results in a very large increase in the availability of IP addresses and creates a lot of advantages. ii) End to End Connectivity: IPv6 eliminates the need for NAT which results in better connectivity in peer-peer networks. iii) Interoperability: IPv6 promotes interoperability between different IPv6 implementations. iv) Built-in Security: IPv6 provides authentication and encryption.	**2M** ***Any Two Points***

2.		**Attempt any THREE of the following:**	**12**
	(a)	**Describe flow control under SCTP.**	**4M**
	Ans.	**Flow control under SCTP** Flow control in SCTP is similar to that in TCP. Like TCP, SCTP executes flow control to prevent overwhelming the receiver. In SCTP, we need to handle two units of data, the byte and the chunk. The values of rwnd and cwnd are expressed in bytes; the values of TSN and acknowledgments are expressed in chunks. Current SCTP implementations still use a byte-oriented window for flow control. **Receiver Site:** The receiver has one buffer (queue) and three variables. The queue holds the received data chunks that have not yet been read by the process. The first variable holds the last TSN received,cum TSN. The second variable holds the available buffer size; winsize. The third variable holds the last accumulative acknowledgment, last ACK. The following figure shows the queue and variables at the receiver site.  When the site receives a data chunk, it stores it at the end of the buffer (queue) and subtracts the size of the chunk from winSize. The TSN number of the chunk is stored in the cumTSN variable. 2. When the process reads a chunk, it removes it from the queue and adds the size of the removed chunk to winSize (recycling). 3. When the receiver decides to send a SACK, it checks the value of lastAck; if it is less than cumTSN, it sends a SACK with a cumulative TSN number equal to the cumTSN. It also includes the value of winSize as the advertised window size. **Sender Site:** The sender has one buffer (queue) and three variables: curTSN, rwnd, and inTransit, as	***Diagram 2M Explanation 2M***

		shown in the following figure. We assume each chunk is 100 bytes long. The buffer holds the chunks produced by the process that either have been sent or are ready to be sent.	

The first variable, curTSN, refers to the next chunk to be sent. All chunks in the queue with a TSN less than this value have been sent, but not acknowledged; they are outstanding. The second variable, rwnd, holds the last value advertised by the receiver (in bytes). The third variable, inTransit, holds the number of bytes in transit, bytes sent but not yet acknowledged. The following is the procedure used by the sender.



1. A chunk pointed to by curTSN can be sent if the size of the data is less than or equal to the quantity rwnd – iNTransit. After sending the chunk, the value of curTSN is incremented by 1 and now points to the next chunk to be sent. The value of inTransit is incremented by the siz of the data in the transmitted chunk.
2. When a SACK is received, the chunks with a TSN less than or equato the cumulative TSN in the SACK are removed from the queue and discarded. The sender does not have to worry about them anymore The value of inTransit is reduced by the total size of the discarded chunks. The value of rwnd is updated with the value of the advertised window in the SACK.

(b) **Explain ICMP protocol ? Describe the header format of ICMP.** **4M**

Ans

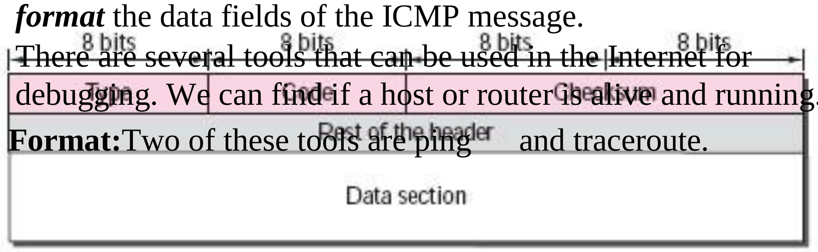
The Internet Control Message Protocol (ICMP) supports the unreliable and connectionless Internet Protocol (IP).

- ICMP messages are encapsulated in IP datagrams. There are two categories of ICMP messages: error-reporting and query messages.The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet. The
- query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.
- The checksum for ICMP is calculated using both the header and the data fields of the ICMP message.
- There are several tools that can be used in the Internet for debugging. We can find if a host or router is alive and running. Two of these tools are ping and traceroute.

2M icmp protocols

2M header format

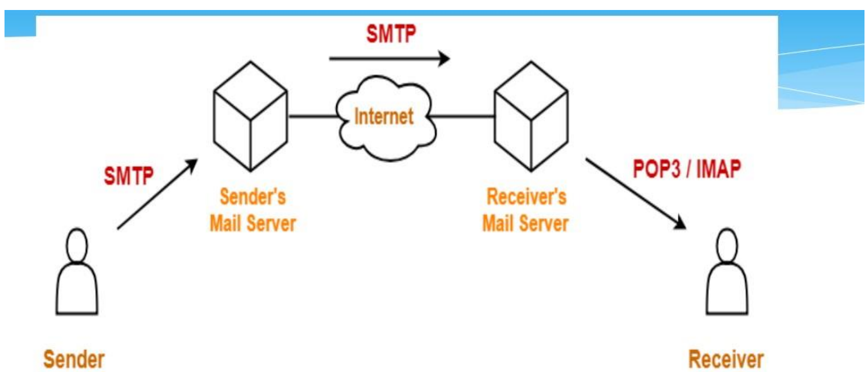
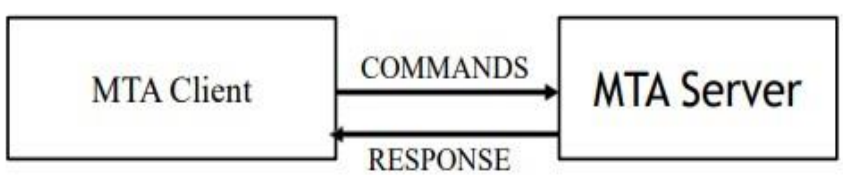
Header Format:



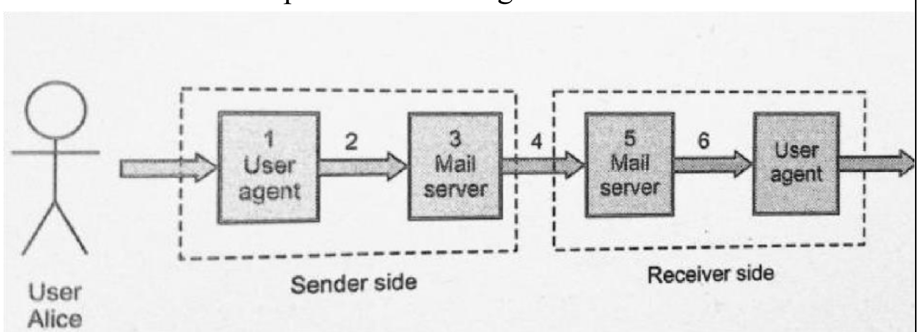
An ICMP message has an 8-byte header and a variable-size data section. Although the general format of the header is different for each message type, the first 4 bytes are common to all. As Figure shows,

- The first field, ICMP type, defines the **type** of the message.
- The **code field** specifies the reason for the particular message type.
- The last common field is the **checksum field** for checking errors
- The rest of the header is specific for each message type.
- The data section in error messages carries information for finding the original packet that had the error. In query messages, the data section carries extra information based on the type of the
- Query.

	(c)	**Describe SMTP with suitable diagram**	**4M**

	Ans.	• It is an application layer protocol of TCP/IP model. • It transfer messages from sender's mail servers to receivers mail server. • SMTP interacts with local mail system and not user. • SMTP uses a TCP socket on port 25 to transfer email reliably from client to server. • Email is temporarily stored on the local and eventually transferred directly to receiving server. • It is simple ASCII protocol.  COMMANDS & RESPONSE SMTP uses commands and response to transfer message between  MTA client and MTA server	***Diagram 2M Explanation 2M***

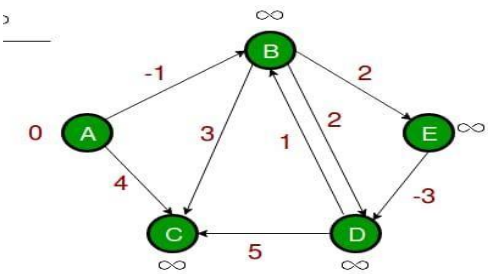
		❑ SMTP Commands: 1. HELO: Used by client to identify itself. 2. MAIL FROM: Identify sender. 3. RCPT TO: Identify intended recipient. 4. DATA: Send actual message. 5. QUIT: Terminate the message. 6. RSET: Reset the connection 7. VRFY: Verify the add of recipient 8. HELP: Mail Example: Scenario: Alice sends message to Bob 1. Alice uses user agents (UA) to compose message and send to bob@technical.org. 2. Alice UA sends message to her mail server, message placed in	

		message queue. 3. Client side of SMTP opens TCP connection with Bob's mail server. 4. SMTP client sends Alice message over TCP connection. 5. Bob's mail server places the message in Bob's mailbox.  6. Bob invokes his user agent to read message.	

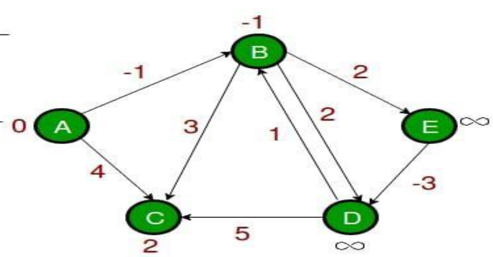
	(d)	**a) For the block of IPv4 address given below build subnet mask, broadcast Address and Number of Hosts possible.** **I. 10.0.199.237/22** **II. 192.168.1487/26**	**4M** ***2M for each correct answer***
	Ans	**i. 10.0.199.237/22** Subnet Mask 255.255.252.0 Network Address 10.0.199.237= 00001010.00000000.11000111.11101101 AND 255.255.252.0=11111111.11111111.11111100.00000000 --- 10.0.196.0 =00001010.00000000. 11000100.00000000 No of host 2^{10} -2=1022 Broadcast Address 10.0.199.255 Range IP Address 10.0.196.1 - 10.0.199.254 **ii. 192.168.14.87/26** Subnet Mask 255.255.255.192 Network Address 192.168.14.87= 11000000.10101000. 00001110.01010111 AND 255.255.255.192=11111111.11111111.11111111.11000000 --- 192.168.14.64 =11000000. 10101000. 00001110.01000000 No of host 2^6 -2=62 Broadcast Address 192.168.14.127 Range Of IP 192.168.14.65 - 192.168.14.126	

MODEL ANSWER

3.		**Attempt any THREE of the following:**	**12**
	(a)	**Explain distance vector routing with suitable example.**	**4M**
	Ans.	A distance-vector r outing (DVR) protocol requires that a router inform its neighbo rs of topology changes periodically. known as the old istorically Bellman Ford algo RPANET routing algorithm (or known as the information wi thm). Routing table are updated by exchanging doesn't have any h the neighbours. Distance vector routing utilization is lower erarchical structure. CPU and memory less due to local sh han link state routing. Bandwidth required is vector routing are ring, small packet and no flooding. Distance convergence asier to configure. DVR are the slow protoc **EXAMPLE**	***2m explanati on 2m for correct***

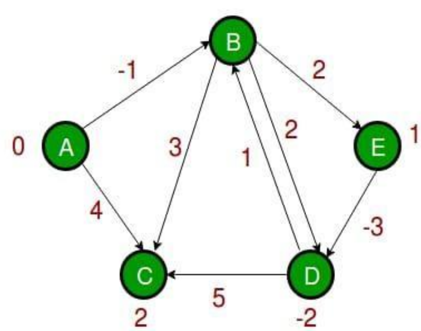
		ol. Its count to infinity problems. **Step 1:** ...en source vertex be 0. Initialize all distances as infinite, except ... distance to the source itself. Total number of ... ie graph is 5, so all edges must be processed 4 times.  ...dges are processed in the following order: (B, E), (D, B), (B, D), (A, B), (A, C), (D, C), (B, C), (E, D). We get the ... when all edges are processed the first time. ... s initial distances. The second row shows ...ges (B, E), (D, B), (B, D) and (A, B) are processed. The third row shows ... when (A, C) is processed. The ... when (D, C), (B, C) and (E, D) are processed.		*example*

A	B	C	D	E
0	∞	∞	∞	∞
0	-1	∞	∞	∞
0	-1	4	∞	∞
0	-1	2	∞	∞



Step 3: The first iteration guarantees to give all shortest paths which are at most 1 edge long. We get the following distances when all edges are processed second time (The last row shows final values.

A	B	C	D	E
0	∞	∞	∞	∞
0	-1	∞	∞	∞
0	-1	4	∞	∞
0	-1	2	∞	∞
0	-1	2	∞	1
0	-1	2	1	1
0	-1	2	-2	1



Step 4: The second iteration guarantees to give all shortest paths which are at most 2 edges long. The algorithm processes all edges 2 more times. The distances are minimized after the second iteration, so third and fourth iterations don't update the distances.

	(b) **Ans**	**Describe the working of TELNET**. For TCP / IP networks like the Internet, Telnet is a terminal emulation program. The software Telnet runs on your system and links your Personal Computer to a network server. It allows a user to access an account or computer remotely. **WORKING** It makes available users by an interactive and bidirectional textoriented message system exploit an effective terminal connection which is much more than 8 byte. User data is sprinkled in the band long with telnet control information above the TCP. It helps to achieve some functions in a remote manner. The user joins the server beside using the TCP protocol, so that means like the other side connection is also established using the telnet hostname. These commands are used on the server by the corresponding user to achieve the need task. These commands are used to end a telnet session or logoff a session or a user. Currently, both virtual terminal and terminal emulators can be used for telnet, which is fundamentally a modern computer that converses by means of the identical Telnet protocol. This command helps telnet protocol to achieve communication with a remote device and mainly various other OS also provides a large amount of support for these systems **SYNTAX** telnet hostname port	**4M** ***4M for correct working***

<table>
<tr><td></td><td>(c)
Ans</td><td>List UDP services and UDP application (any 4 each).
Services offered by the UDP are a s follows:
Process to process port to port transmission of segment.
Connectionless and minimum overhead Protocol
Fast and simple transmission
No flow and error control application using UDP services are responsible for providing them.
UDP encapsulates and decapsulates the message.
UDP application
Domain Name Services.
Simple Network Management Protocol.
Trivial File Transfer Protocol.
Routing Information Protocol.
Kerberos.</td><td>4M

2M for Services

2M for application</td></tr>
<tr><td></td><td>(d)

Ans</td><td>Find out the error, if any in the following IPv4 addresses. a. 111.56.054.78
b. 222.34.7.8.20
c. 75.45.301.14
d. 11100101.23.14.67<table><tr><th>Question</th><th>Answer</th></tr><tr><td>111.56.054.78</td><td>There must be no leading zero (054)</td></tr><tr><td>222.34.7.8.20</td><td>4 octets only in IPv4 address</td></tr><tr><td>75.45.301.14</td><td>Range of each octet is between o and 255</td></tr><tr><td>11100101.23.14.67</td><td>A mixture of binary and dotted decimal notation is not allowed</td></tr></table></td><td>4M

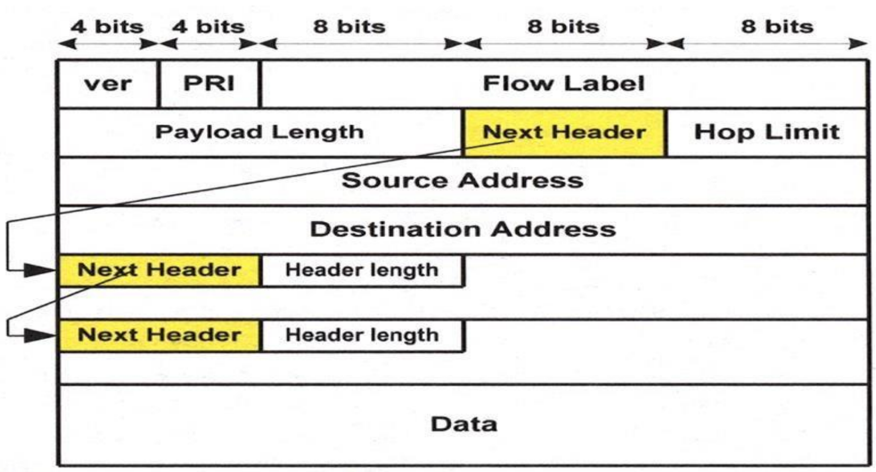
1M EACH</td></tr>
</table>

SUMMER – 2023 EXAMINATION
MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

4.		**Attempt any THREE of the following:**	**12**
	(a)	**Distinguish between SMTP & POP3 protocol.**	**4M**
	Ans.	(see table below)	***Any 4 points 1M each***

SMTP	POP3
SMTP stands for SIMPLE MAIL TRANSFER PROTOCOL & is also called Push Protocol.	POP3 stands for POST OFFICE PROTOCOL VERSION 3 & is also called a Pop Protocol.
SMTP is used for Sending emails.	POP3 is used to retrieve the emails.
SMTP transfers Email from Sender's Device to the mailbox on the recipient's server.	POP3 retrieves Emails from the mailbox on the receipting's server to their device.
It is a message transfer Agent. SMTP has two MTAS.	It is a message access Agent. POP3 has two MAAS.
SMTP uses Ports 25, 465 & 587.	POP3 uses Ports 110 or 995.

	(b) **Ans**	**Draw & explain IPv6 packet format.** IPV6 PACKET FORMAT-  1. **Version:** This 4-bits field defines the version number of IP. The value is 6 for IPV6. 2. **Priority:** This 4-bits priority field defines the priority of packet with respect to traffic congestion. 3. **Flow Label:** It is 24 bits field that is designed to provide	**4M** ***2M for Diagram & 2M for Explanation***

special handling for a particular flow of data.

4. **Payload Length:** The 16 bits payload length field defines the length of the IP datagram excluding the base header.
5. **Next Header:** It is an 8 bits field defining the header that follows the base header in datagram.
6. **Hop Limit:** This 8 bits field serves the same purpose as the TTL field in IPV4.
7. **Source Address:** The source address field is a 128 bits internet address that identifies the original.
8. **Destination Address:** It is 128 bits internet address that usually identifies the final destination of datagram.
9. **Payload:** Is combination of zero or more extension headers(options) which is followed by data from other

protocols such as UDP, TCP etc.

EXTENSION HEADERS

• The length of the base header is fixed at 40 bytes.
• Types of extension headers are:

1. Hop by Hop option
2. Source routing
3. Fragmentation
4. Authentication
5. Encrypted security payload
6. Destination option

1. **Hop by Hop options** is used when the source needs to pass information to all the routers visited by the datagram.
2. **Source routing** extension header combines the concept of strict source route & the loose source route options

of IPV4.

3. **Fragmentation** is the same as that in IPV4. in IPV6 only the original

source can be fragment.

4. **Authentication** header has a dual purpose: it validates the message

sender & ensure the integrity of data.

5. **Encrypted security Payload** is an extension that provides confidentiality & guards.
6. **Destination option** is used when the service needs to pass information to destination only, intermediate routers are not permitted access to this information.

SUMMER – 2023 EXAMINATION
MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

(c) Ans. **Differentiate between RIP & OSPF routing protocol.** **4M**

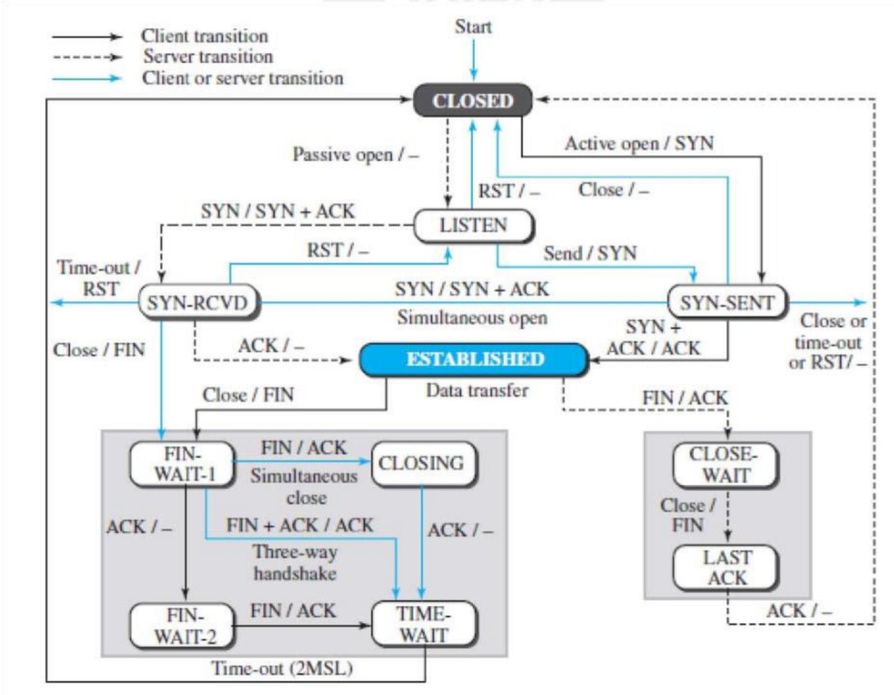
Any 4 points 1M each

RIP	OSPF
RIP Stands for Routing Information Protocol.	OSPF stands for Open Shortest Path First.
RIP works on the Bellman-Ford algorithm.	OSPF works on Dijkstra algorithm.
It is a Distance Vector protocol and it uses the distance or hops count to determine the transmission path.	It is a link-state protocol and it analyzes different sources like the speed, cost and path congestion while identifying the shortest path.
It is used for smaller size organizations.	It is used for larger size organizations in the network.
It allows a maximum of 15 hops.	There is no such restriction on the hop count.
It is not a more intelligent dynamic routing protocol.	It is a more intelligent routing protocol than RIP.
The networks are classified as areas and tables here.	The networks are classified as areas, sub-areas, autonomous systems, and backbone areas here.
Its administrative distance is 120.	Its administrative distance is 110.
RIP uses UDP(User Datagram Protocol) Protocol.	OSPF works for IP(Internet Protocol) Protocol.

It calculates the metric in terms of Hop Count.	It calculates the metric in terms of bandwidth.
In RIP, the whole routing table is to be broadcasted to the neighbors every 30 seconds by the routers.	In OSPF, parts of the routing table are only sent when a change has been made to it.
RIP utilizes less memory compared to OSPF but is CPU intensive like OSPF.	OSPF device resource requirements are CPU intensive and memory
It consumes more bandwidth because of greater network resource requirements in sending the whole routing table.	It consumes less bandwidth as only part of the routing table is to send.

SUMMER – 2023 EXAMINATION
MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

	(d) Ans.	**Describe the state transaction of TCP.** To observe the events happening during connection establishment, connection termination, and data transfer, TCP is specified as the finite state machine (FSM) as shown in Figure 4.4.1. Here two FSMs used by the TCP client and server combined in one diagram. The rounded-corner rectangles represent the states. The transition from one state to another is shown using directed lines. Each line has two strings separated by a slash. The first string is the input, what TCP receives. The second is the output, what TCP sends.  **Fig4.4.1: State transition diagram.** The dotted black lines in the figure represent the transition that a server normally goes through; the solid black lines show the transitions that a client normally goes through.In some situations, a server transitions through a solid line or a client transitions through a dotted line. The colored lines show special situations. The roundedcorner rectangle marked ESTABLISHED has two sets of	**4M** ***2M for Diagram & 2M for Explanation***

		states, a set for the client and another for the server, that are used for flow and error control. Consider the scenario. Figure 4.4.2 shows the state transition diagram for this scenario. The client process issues an active open command to its TCP to request a connection to a specific socket address.	

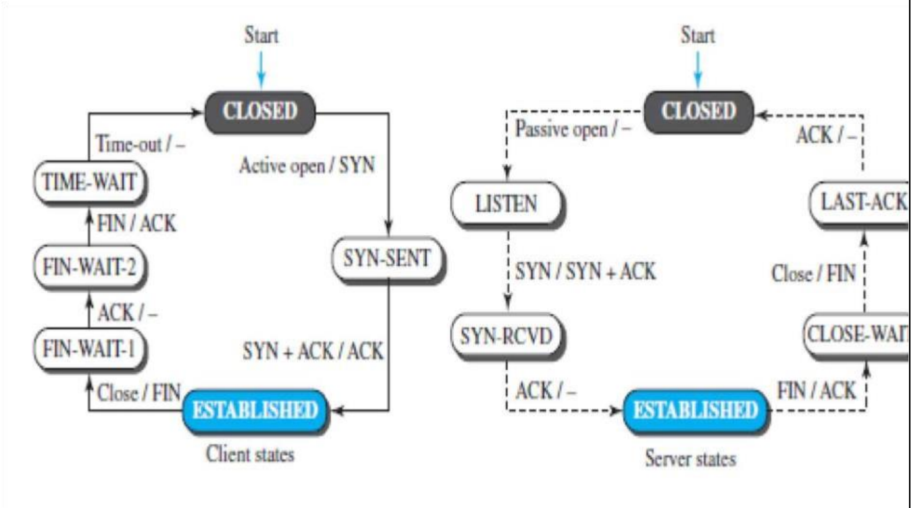


Fig4.4.2: State transition diagram.

TCP sends a SYN segment and moves to the SYN-SENT state. After receiving the SYN +ACK segment, TCP sends an ACK segment and goes to the ESTABLISHED state. Data are transferred, possibly in both directions, and acknowledged. When the client process has no more data to send, it issues a command called an active close. The TCP sends a FIN segment and goes to the FINWAIT-1 state. When it receives the ACK segment, it goes to the FINWAIT-2 state. When the client receives a FIN segment, it sends an ACK segment and goes to the TIME-WAIT state.The client remains in this state for 2 MSL .MSL is the maximum time a TCP segment is expected to live, or stay in the network.When the corresponding timer expires, the client goes to the CLOSED state.The server process issues a passive open command. The server TCP goes to the LISTEN state and remains there passively until it receives a SYN segment.

The TCP then sends a SYN +ACK segment and goes to the SYNRCVD state, waiting for the client to send an ACK segment. After receiving the ACK segment, TCP goes to the ESTABLISHED state, where data transfer can take place. TCP remains in this state

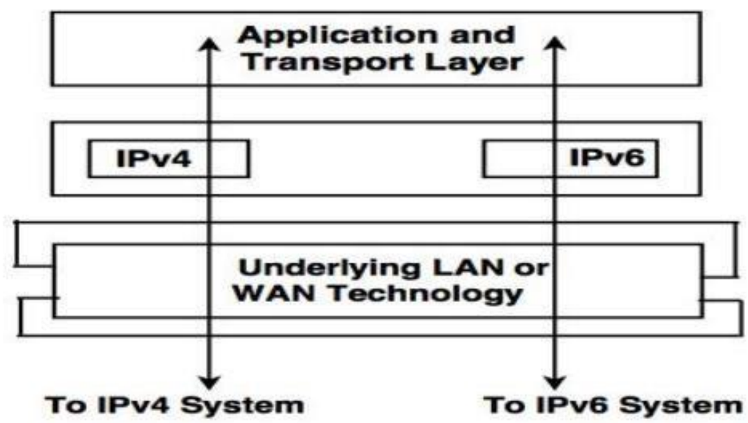
		until it receives a FIN segment from the client signifying that there are no more data to be exchanged and the connection can be closed.The server, upon receiving the FIN segment, sends all queued data to the server with a virtual EOF marker, which means that the connection must be closed. It sends an ACK segment and goes to the CLOSEWAIT state, but postpones acknowledging the FIN segment received from the client until it receives a passive close command from its process. After receiving the passive close command, the server sends a FIN segment to the client and goes to the LASTACK state, waiting for the final ACK. When the ACK segment is received from the client,the server goes to the CLOSE state.	

SUMMER – 2023 EXAMINATION
MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

	(e) **Ans.**	**Explain the process of resolving the given host name into IP address using DNS.** You can find the hostname of any computer with a public IP address by passing the address to any Domain Name System (DNS) server. However, since the computers on a small business network have private IP addresses, you can only discover their hostnames if the network has a local DNS server. To discover the hostname of a computer with a private IP address and no local DNS server, you need to use a Windows utility to query the host itself. **Querying DNS** Click the Windows Start button, then "All Programs" and "Accessories." Right-click on "Command Prompt" and choose "Run as Administrator." Type "nslookup %ipaddress%" in the black box that appears on the screen, substituting %ipaddress% with the IP address for which you want to find the hostname. Find the line labeled "Name" underneath the line with the IP address you entered and record the value next to "Name" as the hostname of the computer	**4M** ***4M for Explanation***

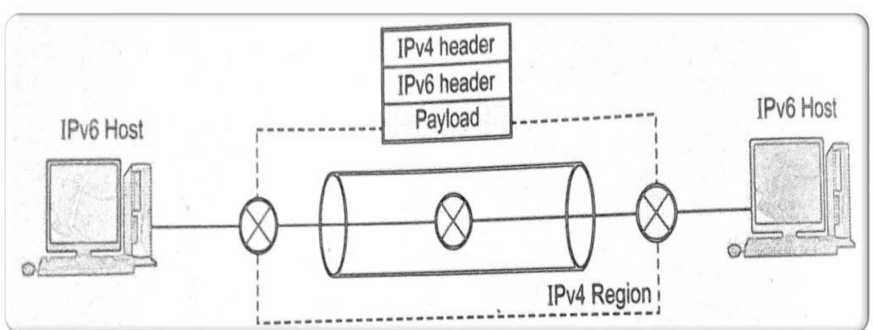
5.		**Attempt any two of the following:**	**12M**
	(a)	**Explain the process of transition form ipv4 to ipv6.**	**6M**
	Ans	TRANSITION FROM IPV4 TO IPV6 ➢ There are 3 strategies have devised by IFTF to help transition. **1. Dual Stack 2. Tunnelling 3. Header Translation** ➢ **Dual Stack:** 1. All the host must run IPV4 and IPV6 simultaneously until all the internet uses IPV6. 2. To determine which version to use when sending packet to destination, the source host queries the DNS. 3. If the DNS returns IPV4 address, the source host sends an IPV4 packet. If DNS returns an IPV6 address the source host sends an IPV6 packet.	***2M each for Correct process transition***



Dual Stack

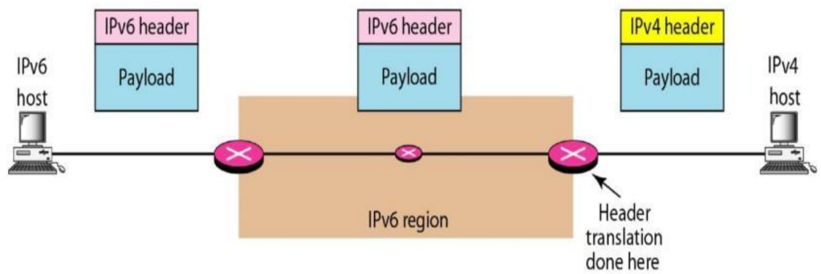
➢ **Tunnelling:**

1. When two computers using IPV6 want to communicate with each other & the packet must pass through a region that uses IPV4.
2. The IPV6 packet is encapsulated in a IPV4 packet when it enter the region & leaves its capsule when it exits the region.



➢ **Header Translation:**

1. It is used when some of the system uses IPV4. the sender wants to use IPV6, but the receiver don't understand IPV6
2. The header format must be totally changed through header translation. The header of IPV6 packet is converted to IPV4 header.


IPv6 header
Payload
IPv6 header
Payload
IPv4 header
Payload
IPv6
host
IPv4
host
IPv6 region
Header
translation
done here

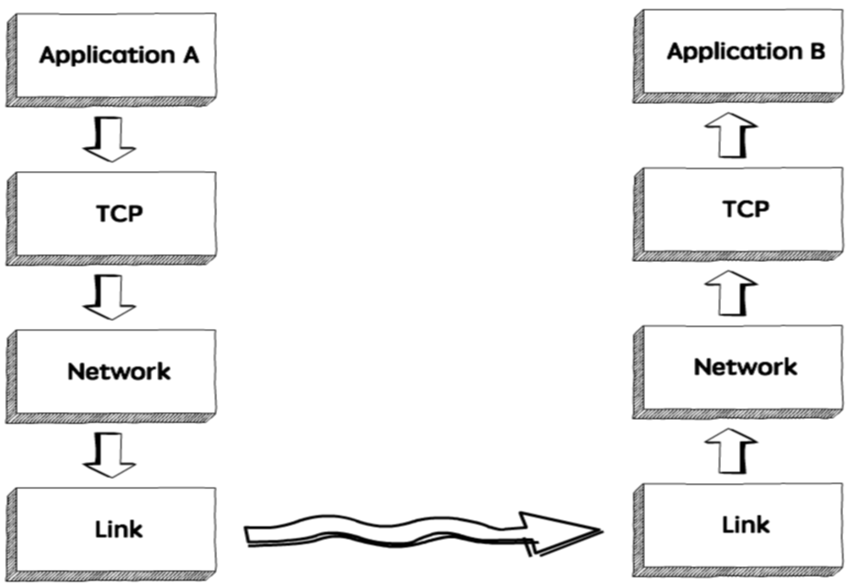
SUMMER – 2023 EXAMINATION
MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

	(b)	**Explain TCP with respect to flow control and error control.**	**6M**

Ans.

TCP Flow Control is a protocol designed to manage the data flow between the user and the server. It ensures that there is a specific bandwidth for sending and receiving data so the data can be processed without facing any major issues. In order to achieve this, the TCP protocol uses a mechanism called the sliding window protocol.



Each explanation of flow control 3M and error control 3M

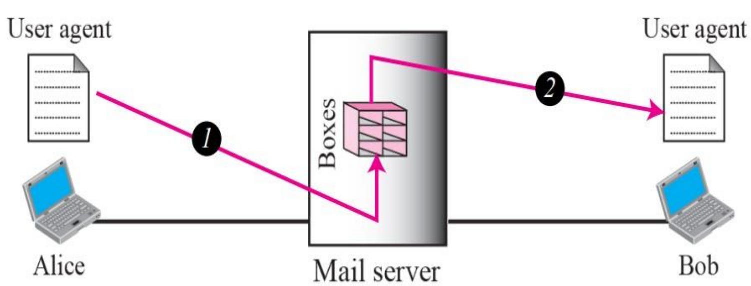
Error control in TCP is mainly done through the use of **three simple techniques** :

1. **Checksum –** Every segment contains a checksum field which is used to find corrupted segments. If the segment is corrupted, then that segment is discarded by the destination TCP and is considered lost.
2. **Acknowledgement –** TCP has another mechanism called acknowledgement to affirm that the data segments have been delivered. Control segments that contain no data but have sequence numbers will be acknowledged as well but ACK segments are not acknowledged.
3. **Retransmission –** When a segment is missing, delayed to

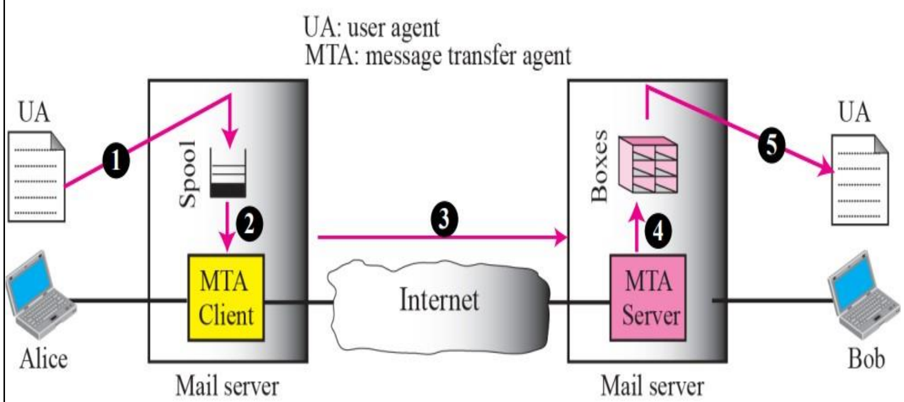
deliver to a receiver, corrupted when it is checked by the receiver then that segment is retransmitted again. Segments are retransmitted only during two events: when the sender receives three duplicate acknowledgements (ACK) or when a retransmission timer expires.

- **Retransmission after RTO:** TCP always preserves one retransmission time-out (RTO) timer for all sent but not acknowledged segments. When the timer runs out of time, the earliest segment is retransmitted. Here no timer is set for acknowledgement. In TCP, the RTO value is dynamic in nature and it is updated using the round trip time (RTT) of segments. RTT is the time duration needed for a segment to reach the receiver and an acknowledgement to be received by the sender.
- **Retransmission after Three duplicate ACK segments:** RTO method works well when the value of RTO is small. If it is large, more time is needed to get confirmation about whether a segment has been delivered or not. Sometimes one segment is lost and the receiver receives so many out-of-order segments that they cannot be saved. In order to solve this situation, three duplicate acknowledgement method is used and missing segment is retransmitted immediately instead of retransmitting already delivered segment. This is a fast retransmission because it makes it possible to quickly retransmit lost segments instead of waiting for timer to end.

	(c) Ans	**Describe the architecture of e-mail system using four scenario.** To explain the architecture of e-mail, we give four scenarios. We begin with the simplest situation and add complexity as we proceed. The fourth scenario is the most common in the exchange of e-mail. **TCP/IP Protocol Suite 2 Topics Discussed in the Section** • First Scenario • Second Scenario • Third Scenario • Fourth Scenario • **First Scenario**	**6M** ***Correct describtion using scenarios 6M***

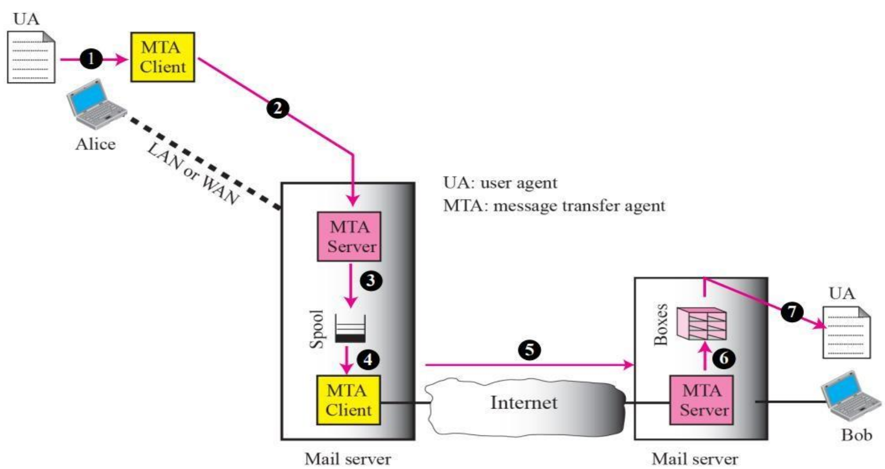


When the sender and the receiver of an e-mail are on the same mail server, we need only two user agents.



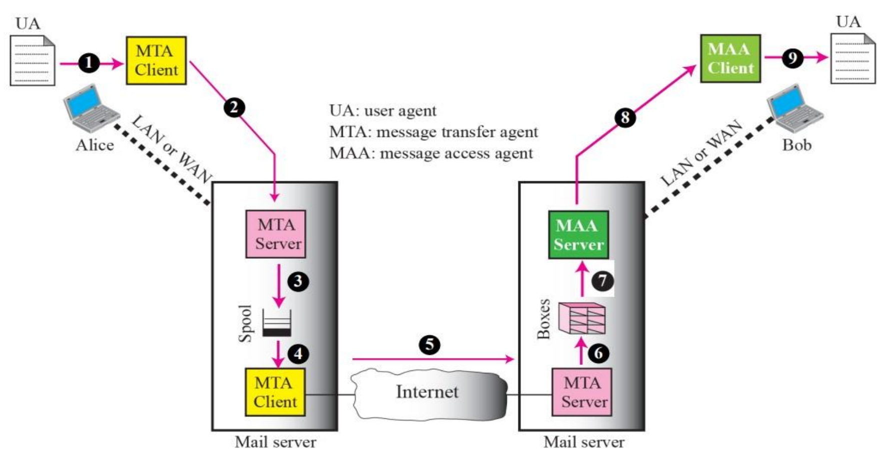
- **Second Scenario**

When the sender and the receiver of an e-mail are on different mail servers, we need two UAs and a pair of MTAs (client and server).



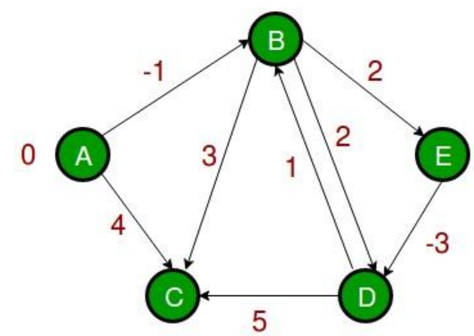
- **Third Scenario**

When the sender is connected to the mail server via a LAN or a WAN, we need two UAs and two pairs of MTAs (client and server).

		• **Fourth Scenario**  When both sender and receiver are connected to the mail server via a LAN or a WAN, we need two UAs, two pairs of MTAs (client and server), and a pair of MAAs (client and server). This is the most common situation today.	

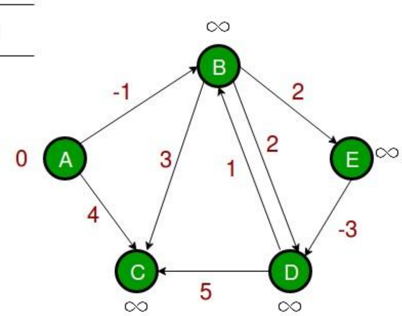
6.		**Attempt any TWO of the following:**	**12**
	(a)	**Explain Bellman Ford algorithm with suitable example**	**6M**
	Ans	**i.** Bellman ford algorithm is a single-source shortest path algorithm. **ii.** This algorithm is used to find the shortest distance from the single vertex to all the other vertices of a weighted graph. **iii.** Various other algorithms are used to find the shortest path, like the Dijkstra algorithm. **iv.** If the weighted graph contains the negative weight values, then the Dijkstra algorithm does not confirm whether it produces the correct answer or not. **v.** Rule for the algorithm: We will go on relaxing all the edges (n - 1) times where n = number of vertices vi. Relaxing means: If (d(u) + c(u , v) < d(v)) d(v) = d(u) + c(u , v)	***3M for explaination and 3M for example*** ***Any other example shall be considered***

vii. Consider the following example:-



Step 1: Let the given source vertex be 0. Initialize all distances as infinite, except the distance to the source itself. The total number of vertices in the graph is 5, so all edges must be processed 4 times.

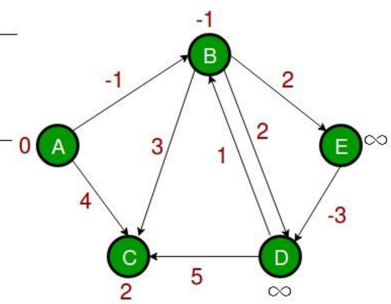
A	B	C	D	E
0	∞	∞	∞	∞



Step 2: Let all edges are processed in the following order: (B, E), (D, B),(B, D), (A, B), (A, C), (D, C), (B, C), (E, D). We get the following distances when all edges are processed the first time. The first row shows initial distances. The second row shows distances when edges (B, E), (D, B), (B, D) and (A, B) are processed. The

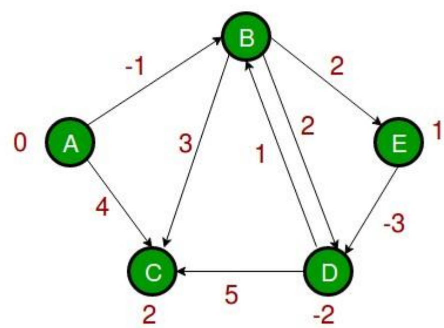
		third row shows distances when (A, C) is processed. The fourth row shows when (D, C), (B, C) and (E, D) are processed.	

A	B	C	D	E
0	∞	∞	∞	∞
0	-1	∞	∞	∞
0	-1	4	∞	∞
0	-1	2	∞	∞



Step 3: The first iteration guarantees to give all shortest paths which are at most 1 edge long. We get the following distances when all edges are processed second time (The last row shows final values).

A	B	C	D	E
0	∞	∞	∞	∞
0	-1	∞	∞	∞
0	-1	4	∞	∞
0	-1	2	∞	∞
0	-1	2	∞	1
0	-1	2	1	1
0	-1	2	-2	1



Step 4: The second iteration guarantees to give all shortest paths which are at most 2 edges long. The algorithm processes all edges 2 more times. The distances are minimized after the second iteration, so third and fourth iterations do not update the distances.

SUMMER – 2023 EXAMINATION
MODEL ANSWER

Subject: Advanced Computer Network **Subject Code:** **22520**

	(b)	**For the IP address given below, find the range of addresses in the following blocks:** **a. 123.56.77.32/29** **b. 200.17.21.128/27** **c. 17.34.16.0/23** **d. 180.34.64.64/30**	**6M**
	Ans.	a. **123.56.77.32/29** • The subnet mask "/29" means the first 29 bits are network bits, and the remaining 3 bits are host bits. • The network address can be obtained by setting the host bits to zero: 123.56.77.32 • The broadcast address can be obtained by setting the host bits to one: 123.56.77.39 • The range of addresses in this block is from 123.56.77.32 to 123.56.77.39 • <u>Range of addresses: 123.56.77.32 to 123.56.77.39</u> b. **200.17.21.128/27** • The subnet mask "/27" means the first 27 bits are network bits, and the remaining 5 bits are host bits. • The network address can be obtained by setting the host bits to zero: 200.17.21.128. • The broadcast address can be obtained by setting the host bits to one: 200.17.21.159. • <u>Range of addresses: 200.17.21.128 to 200.17.21.159</u> c. **17.34.16.0/23:** • The subnet mask "/23" means the first 23 bits are network bits, and the remaining 9 bits are host bits. • The network address can be obtained by setting the host bits to zero: 17.34.16.0. • The broadcast address can be obtained by setting the host bits to one: 17.34.17.255.	**$1\frac{1}{2}$** ***M for each sub-question***

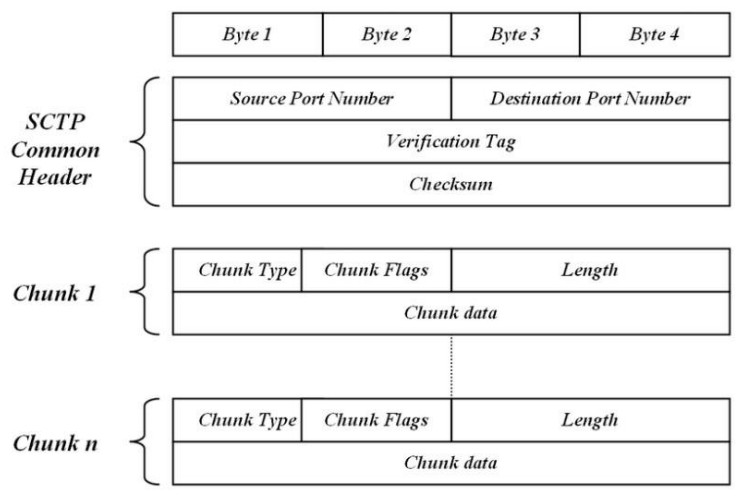
		• Range of addresses: 17.34.16.0 to 17.34.17.255	

		d. **180.34.64.64/30** • The subnet mask "/30" means the first 30 bits are network bits, and the remaining 2 bits are host bits. • The network address can be obtained by setting the host bits to zero: 180.34.64.64. • The broadcast address can be obtained by setting the host bits to one: 180.34.64.67. • <u>Range of addresses: 180.34.64.64 to 180.34.64.67</u>	

(c) **Describe the fields of SCTP packet format. Explain SCTP association establishment process.** **6M**

Ans SCTP transmits data in the form of messages and each message contains one or more packets. The control come before data chunks.

3M for describing fields & 3M for association establishment process



1. **Source and Destination port** number to enable multiplexing of different SCTP associations at the same address.
2. A **32-bit verification tag** that guards against the insertion of an out-of-date or false message into the SCTP association.
3. A **32-bit checksum** for error detection. The checksum can be either a 32-bit CRC checksum or Alder-32 checksum.
4. **Chunk Layout:** A chunk can be either a control chunk or data chunk.

i. **Chunk Type:** This field identifies the type of information contained in the Chunk data field. The value of chunk field ranges from 0 to 254. the value 255 is reserved for future. SCTP consists of one DATA chunk and 12 control chunks.

ii. **Chunk Flag:** The chunk field contains the flag, such as

SUMMER – 2023 EXAMINATION

MODEL ANSWER

U(unordered bit), B(beginning bit), and E(ending bit). Usage of this field depends on the chunk type specified in the chunk type field.

iii. **Chunk Length:** This field represents the size of the fields chunk type, chunk flag, chunk length, and chunk value, in bytes.

5. **SCTP DATA CHUNK:** Data chunks are used to send actual data through the stream and have rather complex headers in some ways, but not really worse than TCP headers in general.

<u>SCTP Association Establishment Process:-</u>

SCTP association startup and shutdown guidelines are described here. SCTP association is comprised of a four-way handshake that takes place in the following order:

i. The client sends an **INIT** signal to the server to initiate an association.

ii. On receipt of the **INIT** signal, the server sends an **INIT-ACK** response to the client. This **INIT-ACK** signal contains a state cookie. This state cookie must contain a Message Authentication Code (MAC), along with a time stamp corresponding to the creation of the cookie, the life span of the state cookie, and the information necessary to establish the association. The MAC is computed by the server based on a secret key only known to it.

iii. On receipt of this **INIT-ACK** signal, the client sends a **COOKIE-ECHO** response, which just echoes the state cookie.

iv. After verifying the authenticity of the state cookie using the secret key, the server then allocates the resources for the association, sends a **COOKIE-ACK** response acknowledging the **COOKIE-ECHO** signal, and moves the association to **ESTABLISHED** state.

		SCTP supports also graceful close of an active association upon request from the **SCTP** user. The following sequence of events occurs: i. The client sends a **SHUTDOWN** signal to the server, which tells the server that the client is ready to close the connection. ii. The server responds by sending a **SHUTDOWN-ACK** acknowledgement. iii. The client then sends a **SHUTDOWN-COMPLETE** signal back to the server.	

		SCTP also supports abrupt close (**ABORT** signal) of an active association upon the request from the **SCTP** client or due to an error in the **SCTP** stack. However, **SCTP** does not support half open connections. More information about the protocol and its internals can be found in RFC 4960.	

SUMMER – 2023 EXAMINATION

MODEL ANSWER

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

SUMMER _ 2023 EXAMINATION
MODEL ANSWER
WINTER – 2023 EXAMINATION Model Answer – Only for the Use of RAC Assessors

Subject Name: **Advanced Computer Network** **Subject Code:** 22520

Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills.
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.
8) As per the policy decision of Maharashtra State Government, teaching in English/Marathi and Bilingual (English + Marathi) medium is introduced at first year of AICTE diploma Programme from academic year 2021-2022. Hence if the students write answers in Marathi or bilingual language (English +Marathi), the Examiner shall consider the same and assess the answer based on matching of concepts with model answer.

Q. No.	Sub Q. N.	Answer	Marking Scheme
1		**Attempt any FIVE of the following:**	**10 M**
	a	**Differentiate between IPv4 and IPv6 on the basis of length and security.**	**2 M**

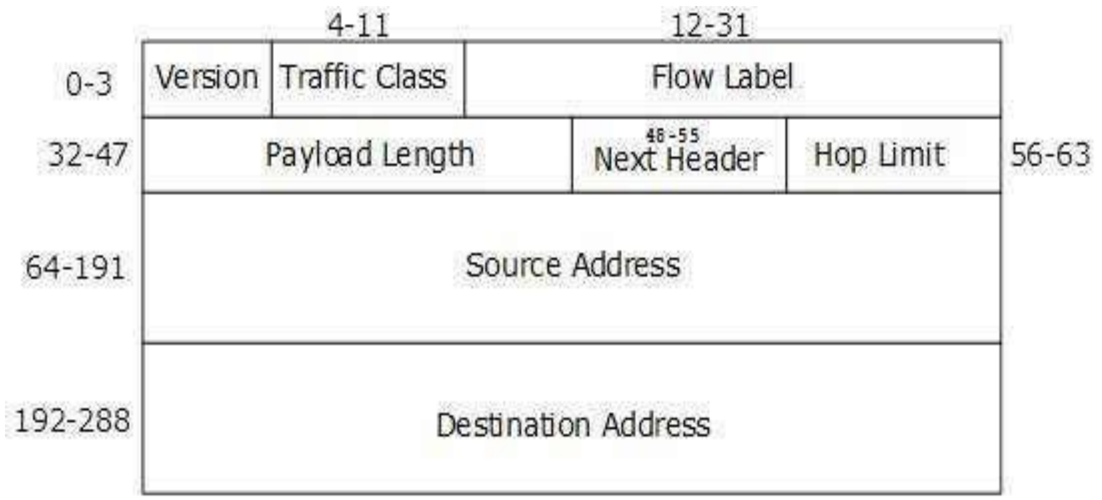
	Ans	<table><tr><th>IPv4</th><th>IPv6</th></tr><tr><td>Addresses are 32 bit (4bytes) in length</td><td>Addresses are 128bits (16 bytes) in length.</td></tr><tr><td>Deployed in 1981</td><td>Deployed in 1999</td></tr><tr><td>Header includes checksum</td><td>Header does not include checksum</td></tr><tr><td>Header includes options</td><td>Optional data is supported as extension header</td></tr><tr><td>Configuration is either manually or through DHCP</td><td>Does not require manual configuration or DHCP</td></tr><tr><td>Address format in dotted decimal notation</td><td>Address format in hexadecimal notation</td></tr><tr><td>Both routers and the sending host fragment packets</td><td>Routers do not support packet fragmentation sending host fragment packets.</td></tr></table>	Any 2 points 1 M each

	b	**State the need of IPv6.**	**2 M**

	Ans	The need of IPv6 are as follows: 1. **Address Space**: IPv6 provides a significantly larger address space compared to IPv4, allowing for the accommodation of the growing number of devices connected to the internet. 2. **Addressing Efficiency**: IPv6 simplifies address assignment and management, eliminating the need for Network Address Translation (NAT) and making subnetting more efficient. 3. **Auto-Configuration**: IPv6 supports stateless address auto-configuration, enabling devices to automatically configure their IPv6 addresses without the need for DHCP (Dynamic Host Configuration Protocol). 4. **Security Improvements**: IPv6 includes features like IPsec (Internet Protocol Security) as a standard, enhancing the security of communications between devices. 5. **Multicast and Any cast**: IPv6 incorporates improved support for multicast communication, enabling efficient one-to-many communication. Anycast is also more easily implemented in IPv6. 6. **Mobility Support**: IPv6 is designed to better support mobile devices, ensuring seamless connectivity as devices move between networks. 7. **Simplified Header Structure:** IPv6 has a simpler and more efficient header structure, reducing processing overhead on networking devices. 8. **Future-Proofing**: As the successor to IPv4, IPv6 is essential for the continued growth of the internet and the proliferation of connected devices, ensuring there are enough unique addresses for future expansion.	Any 2 correct need 1M each
	c	**Elaborate need of domain name system.**	**2 M**
	Ans	1. DNS ensures the internet is not only user-friendly but also works smoothly, loading whatever content we ask for quickly and efficiently. 2. It allows the user to access remote system by entering human readable device hostnames instead of IP address. It translates domain name into IP addresses so browser can load internet resources. 3. It translates human readable domain names into the numerical identifiers associated with networking equipment, enabling devices to be located and connected worldwide. Analogous to a network “phone book,” DNS is how a browser can translate a domain name (e.g., “facebook.com”) to the actual IP address of the server, which stores the information requested by the browser.	Correct explanation 2M
	d	**List any 2 features of TCP.**	**2 M**

	Ans	1) Connection Oriented Protocol 2) Reliable 3) Congestion Control 4) Full Duplex 5) Error Control and Recovery 6) Flow Control	Any 2 correct Feature 1 M each
	e	**List all 4 routing algorithms.**	**2 M**
	Ans	1) Adaptive Routing Algorithm. 2) Link State Routing Algorithm. 3) Distance Vector Routing Algorithm.	1/2 M each algorithm

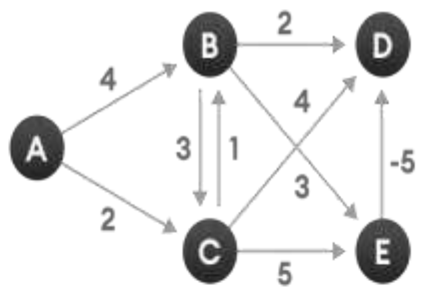
		4) Bellmen Ford Algorithm.	
	f	**Enlist any two services offered by UDP.**	**2 M**
	Ans	1) Process to Process communication 2) Connectionless Service 3) Flow control 4) Error control 5) Checksum	Any 2 correct services 1M each
	g	**State any three phases of mobile IP.**	**2 M**
	Ans	The mobile IP process works in 3 main phases: 1) Agent discovery Phase 2) Agent Registration Phase 3) Tunneling	Correct 3 phases 2M
2		**Attempt any THREE of the following:**	**12 M**
	a	**Describe packet format of IPv6.**	**4 M**

	Ans	 **Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110. **Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. **Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media. **Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. **Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's. **Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link. When the field reaches 0 the packet is discarded. **Source Address** (128-bits): This field indicates the address of originator of the packet.	2M Explanation & 2M Diagram

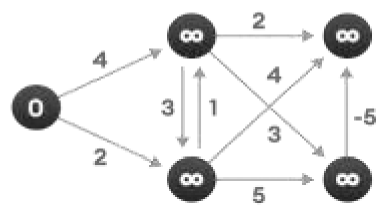
		Destination Address (128-bits): This field provides the address of intended recipient of the packet. **Extension Headers** When Extension Headers are used, IPv6 Fixed Header's Next Header field points to the first Extension Header. If there is one more Extension Header, then the first Extension Header's 'Next-Header' field points to the second one, and so on. The last Extension Header's 'Next-Header' field points to the Upper Layer Header. Thus, all the headers points to the next one in a linked list manner.	
	b	**Explain Bellman Ford algorithm with suitable example.**	**4 M**

	Ans	Dynamic Programming is used in the Bellman-Ford algorithm. It begins with a starting vertex and calculates the distances between other vertices that a single edge can reach. It then searches for a path with two edges, and so on. The Bellman-Ford algorithm uses the bottom-up approach. **Bellman Ford's algorithm** The Bellman-Ford algorithm works by grossly underestimating the length of the path from the starting vertex to all other vertices. **Step 1:** Make a list of all the graph's edges. This is simple if an adjacency list represents the graph. **Step 2:** "V - 1" is used to calculate the number of iterations. Because the shortest distance to an edge can be adjusted V - 1 time at most, the number of iterations will increase the same number of vertices. **Step 3:** Begin with an arbitrary vertex and a minimum distance of zero. Because you are exaggerating the actual distances, all other nodes should be assigned infinity. For each edge u-v, relax the path lengths for the vertices: If distance[v] is greater than distance[u] + edge weight uv, then distance[v] = distance[u] + edge weight uv **Step 4:** If the new distance is less than the previous one, update the distance for each Edge in each iteration. The distance to each node is the total distance from the starting node to this specific node. **Step 5:** To ensure that all possible paths are considered, you must consider alliterations. You will end up with the shortest distance if you do this.	2M Algorith m, 2M Example

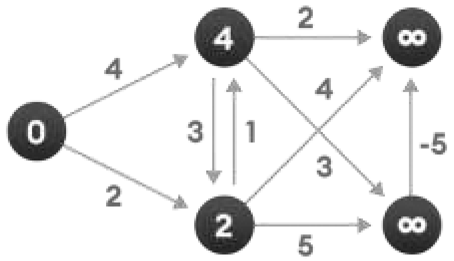
Step 1: Start with the weighted graph



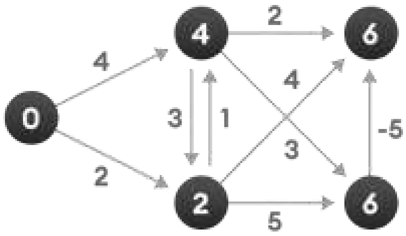
Step 2: Choose a starting vertex and assign infinity path values to all other vertices



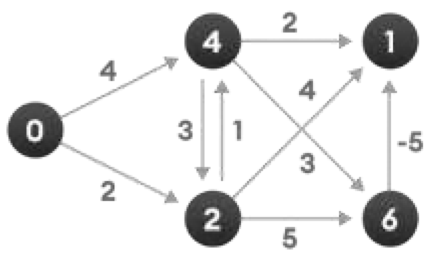
Step 3: Visit each edge and relax the path distances if they are inaccurate



Step 4: We need to do this V times because in the worst case, a vertex's path length might need to be readjusted V times



Step 5: Notice how the vertex at the top right corner had its path length adjusted



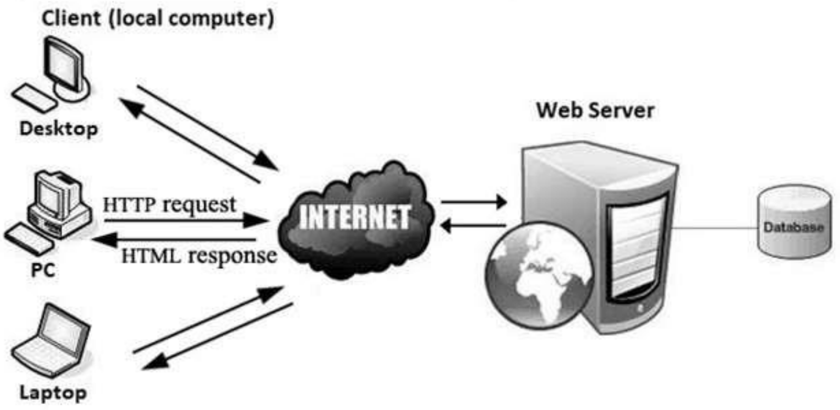
Step 6: After all the vertices have their path lengths, we check if a negative cycle is present

	B	C	D	E
0	∞	∞	∞	∞
0	4	2	∞	∞
0	3	2	6	6
0	3	2	1	6
0	3	2	1	6

	c	**Explain working of world wide web.**	**4 M**

Ans

2M Diagram and 2M Working



The World Wide Web (WWW), also known as the Web, is an interconnected network of web pages and documents accessible through the Internet. Tim Berners-Lee created it in 1989 as a way for researchers to share information through linked documents.

Working of WWW:

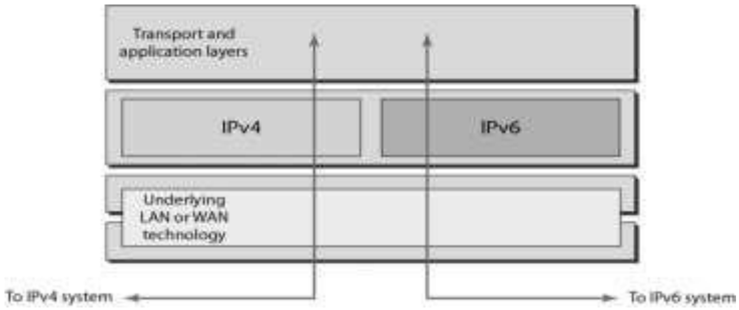
1. A web browser is a software application that allows users to access and view web pages on the Internet.
2. It acts as an interface between the user and the World Wide Web by displaying web pages Web browsers communicate with web servers using the HTTP or HTTPS protocol, which allows users to access websites hosted on remote servers.
3. A web server is a computer program that serves web pages to clients, such as web browsers, upon request. It is responsible for hosting websites, processing HTTP requests, and delivering web content to users online.
4. Hyperlinks one of the key features of the Web is hyperlinks, which allow you to navigate between web pages by clicking on links.
5. Uniform Resource Locators (URLs) Web pages are identified by URLs, which are unique addresses that point to the location of the web page on the Internet.

	d	**If an address in a block given in CIDR classless notation as 64.32.16.8/27 then find the following:** **i. Number of addresses given in block(N)** **ii. The first address** **iii. The last address iv. Find Prefix bit(n)**	**4 M**
	Ans	**1) Number of addresses given in block(N)** The CIDR notation is /27 i.e. 27 bits out of 32 bits are network & remaining 5 bits are host address i.e. **2^5=32** **N=32** **2) The first address** To obtain the first address in block for this we have AND the given address with the network mask n (32-n) network mask=27ones 5 zeros network mask=255.255.255.224 **First address =64.32.16.0** **3) The last address** To obtained last address in the block we have to keep the ledt most 27 bits in the given address as it is and set the remaining 5 bits to 1s **Last address = 64.32.16.31** **4) Find Prefix bit(n)** The CIDR notation “/27” implies the 27 bits are n/w bits so the prefix bit(n)=27	1 M for No. of addresses, 1M- first address, 1M- Last address and 1M- Prefix bit(n)

3		**Attempt any THREE of the following:**	**12 M**
	a	**Differentiate between distance vector routing and link state routing.**	**4 M**
	Ans	(see table below)	Any Four points 1M each

Sr. No.	Distance Vector Routing	Link State Routing
1	Routing tables are updated by exchanging information with the neighbors.	Complete topology is Distributed to every router to update a routing table.
2	It updates full routing table.	It updates only link states.
3	It uses Bellman-Ford algorithm	It uses Dijkstra algorithm.
4	Distance Vector routing doesn't have any hierarchical structure.	Link state routing works best for hierarchical routing design.
5	CPU and memory utilization are lower than Link state routing.	Higher utilization of CPU and memory than distance vector routing.
6	Slow convergence.	Fast convergence.
7	Example protocols are RIP and IGRP.	Example protocols are OSPF and IS-IS.
8	Count to infinity problem	No count to infinity problem

	b	**From below list, explain any two different transition method from IPv4 to IPv6. i) Dual Stack ii) Tunneling iii) Header translation**	**4 M**

	Ans	**1. Dual Stack** In this kind of strategy, a station has a dual stack of protocols run IPv4 and IP simultaneously. To determine which version to use when sending a packet to a destination, the source h queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 pack If the DNS returns an IPv6 address, the source host sends an IPv6 packet.  **Fig. Dual Stack** **2. Tunneling** Tunneling is a strategy used when two computers using IPv6 want to communicate wi each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet must have an IPv4 address. So, the IPv6 packet encapsulated in an IPv4 packet when it enters the region. To make it clear that the IPv4 packet is carrying an IPv6 packet as data the protocol val is set to 41.	2M for any 2 transition methods with diagram

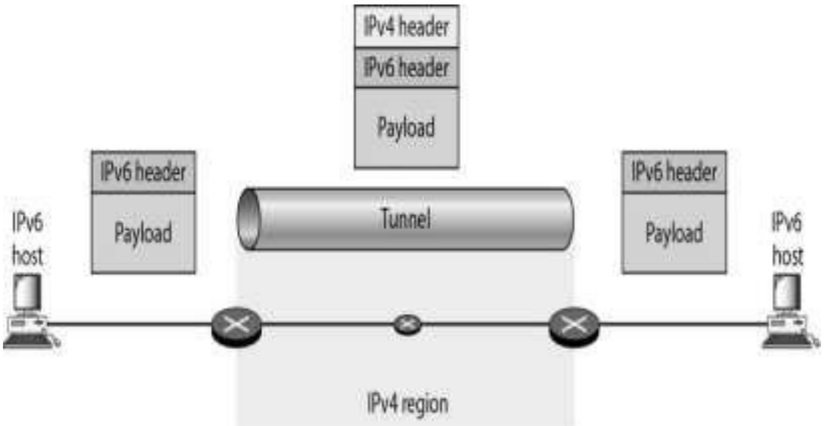


Fig Tunneling

3. Header Translation

In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an Ipv4 header see figure.

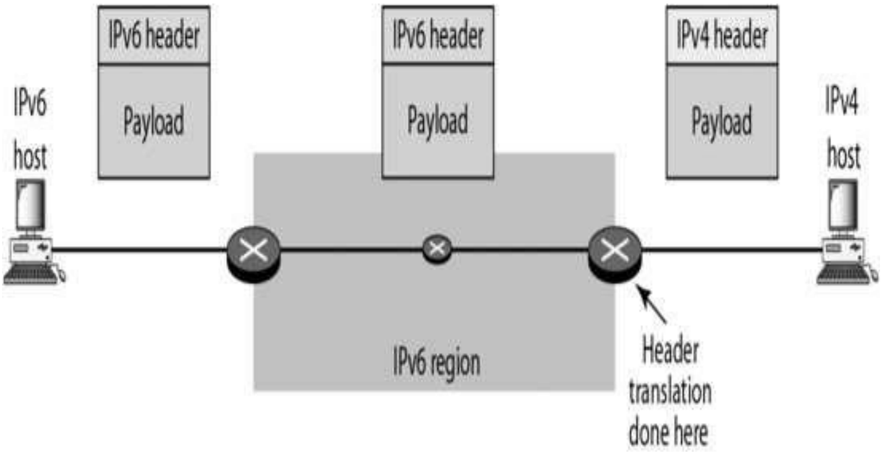
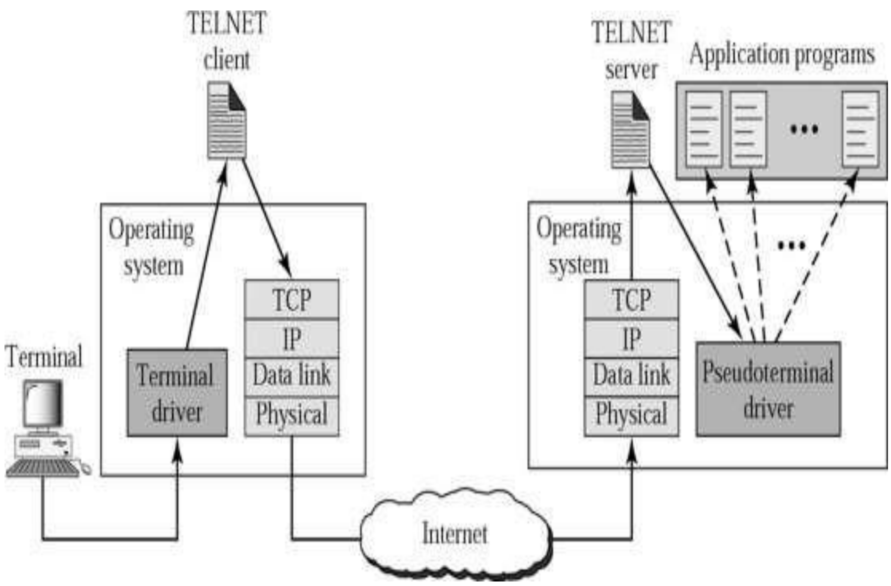


Fig. Header Translation

	c	**Explain the working of TELNET.**	**4 M**

	Ans	**TELNET:** TELNET is an abbreviation for TErminaLNETwork. It is the standard TCP/IP protocol for virtual terminal service. **TELNET Working:** • TELNET is a client-server application that allows a user to log on to a remote machine, giving the user access to the remote system. • The user sends the keystrokes to the terminal driver, where the local operating system accepts the characters but does not interpret them. • A terminal driver correctly interprets the keystrokes on the local terminal or terminal emulator. The characters are sent to the TELNET client, which transforms the characters to a universal character set called network virtual terminal (NVT) characters and delivers them to the local TCP/IP protocol stack. • The commands or text, in NVT form, travel through the Internet and arrive at the TCP/IP stack at the remote machine. • Here the characters are delivered to the operating system and passed to the TELNET server, which changes the characters to the corresponding characters understandable by the remote computer. • However, the characters cannot be passed directly to the operating system because the remote operating system is not designed to receive characters from a TELNET server: It is designed to receive characters from a terminal driver. • A piece of software called a pseudo terminal driver is added which pretends that the characters are coming from a terminal.	Working of Telnet 2M And diagram 2M

		• The operating system then passes the characters to the appropriate application program.  **Fig. Working of TELNET**	
	d	**The dump of a UDP header in hexadecimal format is as follows:** **BC82D00D002B001D** **Obtain the following:** **(i) Source port number** **(ii) Destination port number** **(iii) Total length** **(iv) Packet direction**	**4 M**

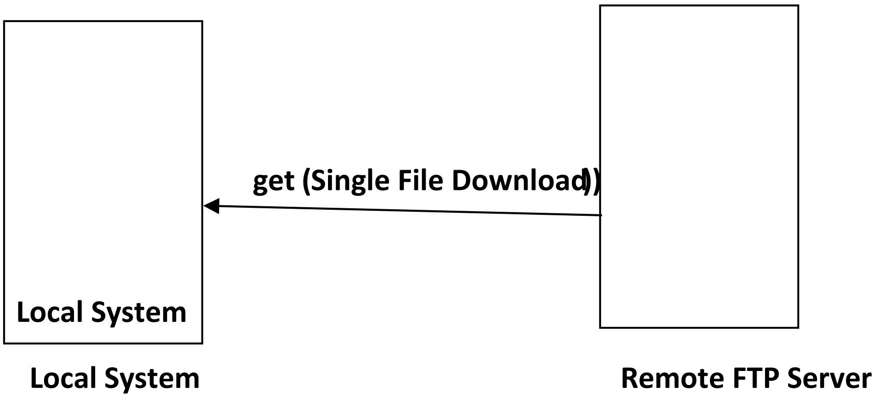
	Ans	Considering hexadecimal format as: **BC82D00D002B001D** The UDP header has four parts, each of two bytes. That means we get the following interpretation of the header. i) Source port number = $BC82_{16}$ = 48258 ii) Destination port number = $D00D_{16}$= 53261 iii) Total length = $002B_{16}$ = 43 bytes iv) Packet direction: The provided dump does not contain information about the packet direction. The UDP header alone does not specify the direction. **OR** Considering hexadecimal format as: **BC82000D002B001D** The UDP header has four parts, each of two bytes. That means we get the following interpretation of the header. i. Source port number = BC8216 = 48258 ii. Destination port number = $000D_{16}$= 13 iii. Total length = 002B16 = 43 bytes iv. Packet direction: Since the destination port number is 13 (well-known port), the packet is from the client to the server.	1 M for Each correct answer
4		**Attempt any THREE of the following:**	**12 M**
	a	**Construct a suitable diagram for each below commands of FTP to show its use i) get ii) mget**	**4 M**

		iii) put iv) mput	
	Ans	(see table below)	Each command and its use with diagram

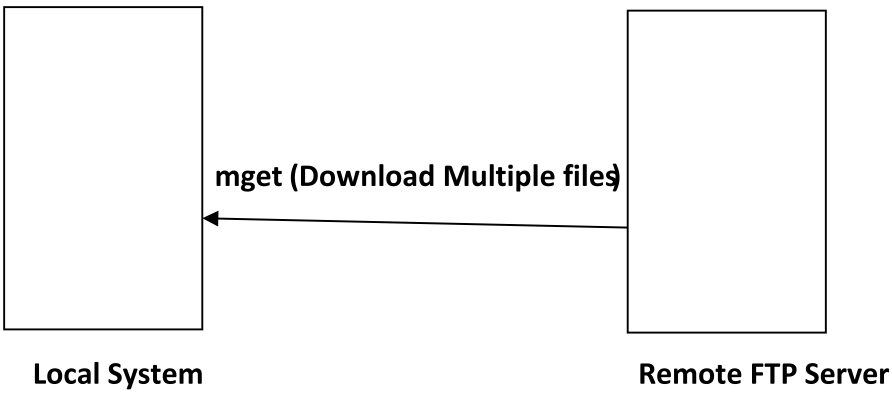
Command	**Purpose**	**Syntax**
get	Download a single file	get<filename>

mget	Download multiple files	mget<filename1 filename2 filename3>	1 M
put	Upload a single file	put<filename>	
mput	Upload multiple files	mput< filename1 filename2 filename3 >	

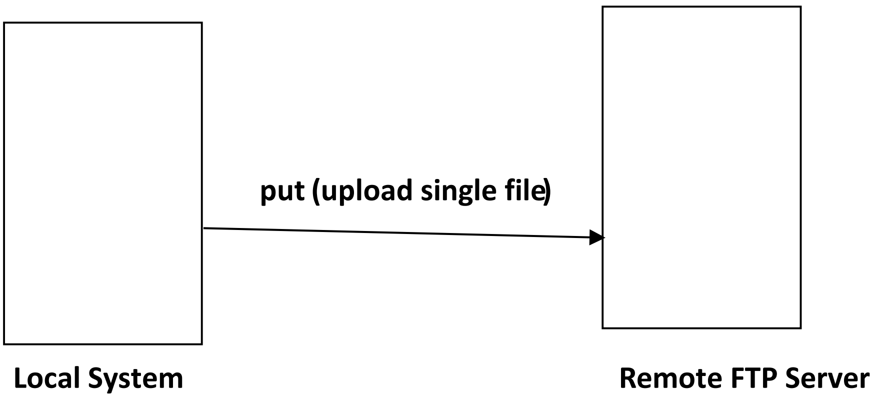
i) get

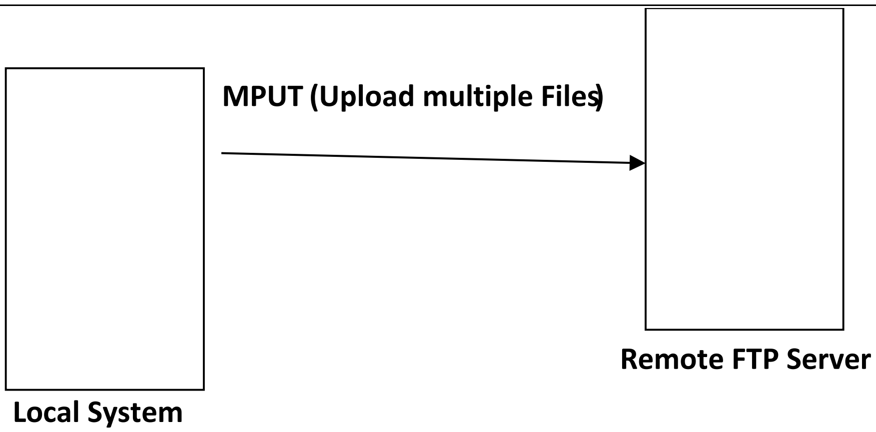


ii) mget



ii) put



		iv)mput 	
	b	**Describe RIP message format in detail.**	**4 M**

Ans

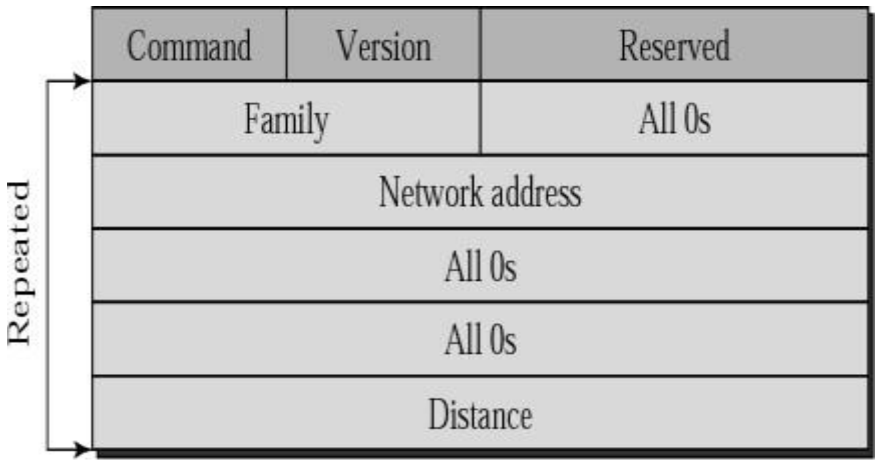
RIP (Routing Information Protocol) message format

•RIP is routing protocol based on Distance Vector Routing algorithm which is an intra domain (interior) routing protocol used inside an autonomous system.

•The metric used by RIP is the distance which is defined as the number of links (networks) that have to be used to reach the destination. For this reason, the metric in RIP is called a hop count.

•Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.

The next node column defines the address of the router to which the packet is to be sent to reach its destination.



- **Command: 8-bit**
  The type of message: request (1) or response (2)
- **Version: 8-bit**
  Define the RIP version
- **All 0s**

This field is not actually used by RFC 1058 RIP; it was added solely to provide backward compatibility with pre-standard varieties of RIP. Its name comes from its defaulted value, zero.

- **Family:**
  16-bit field defines the family of the protocol used. For TCP/IP, value is 2 •
  IP Address Network Address:
  14 bytes n Defines the address of the destination network and

14 bytes for this field to be applicable to any protocol. However, IP currently uses only 4 bytes, the rest are all 0s.

2M Description & 2M Diagram

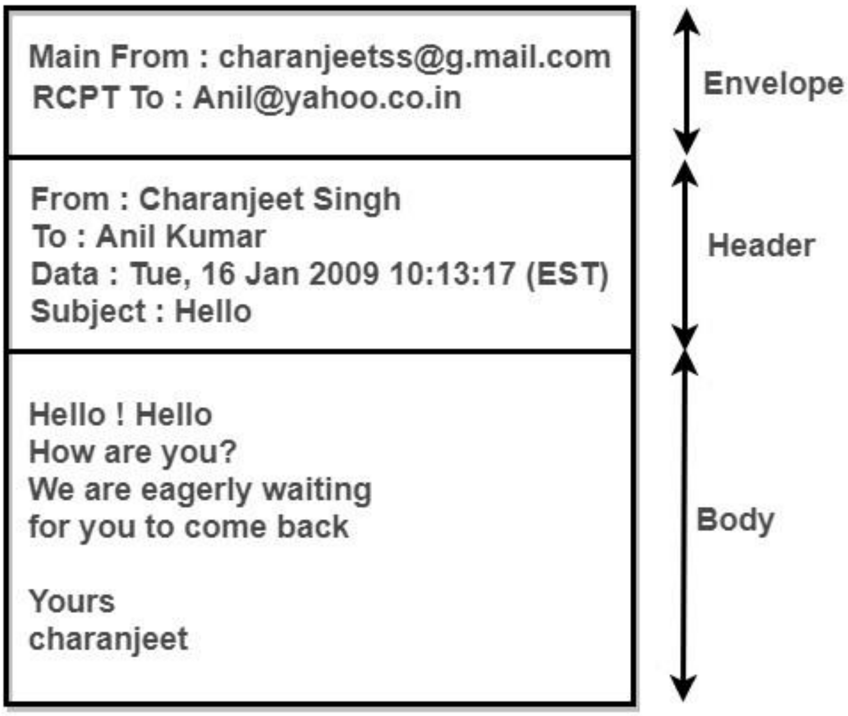
		• **Distance:** 32-bit field defines the hop count from the advertising router to the destination network.	
	c	**Describe the header fields in message format of e-mail system.**	**4 M**

Ans

Electronic Mail (e-mail) is one of the most widely used services of the Internet. This service allows an Internet user to send a message in a formatted manner (mail) to other Internet users in any part of the world. Message in the mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called sender and person who receives mail is called the recipient. Format of E-mail: An e-mail consists of three parts that are as follows:

1. Envelope
2. Header
3. Body

2M Description & 2M for Message format diagram



Header:

The header consists of a series of lines. Each header field consists of a single line of ASCII text specifying field name, colon and value. The main header fields related to message transport are:

1. **To:** It specifies the DNS address of the primary recipient(s).
2. **Cc:** It refers to carbon copy. It specifies address of secondary recipient(s).
3. **BCC:** It refers to blind carbon copy. It is very similar to Cc. The only difference between Cc and Bcc is that it allows user to send copy to the third party without primary and secondary recipient knowing about this.
4. **From:** It specifies name of person who wrote message.

		5. Sender: It specifies e-mail address of person who has sent message. **6. Received:** It refers to identity of sender's, data and also time message was received. It also contains the information which is used to find bugs in routing system. **7. Return-Path:** It is added by the message transfer agent. This part is used to specify how to get back to the sender.	

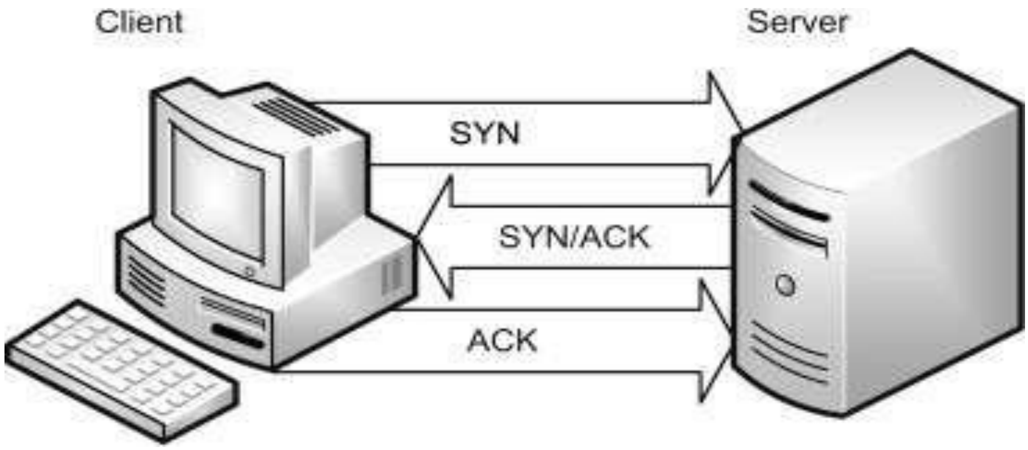
	d	**Compare TCP with UDD on any four points.**	**4 M**
	Ans	**Note: Consider the term UDD as a UDP.**	Any Correct four points 1M each

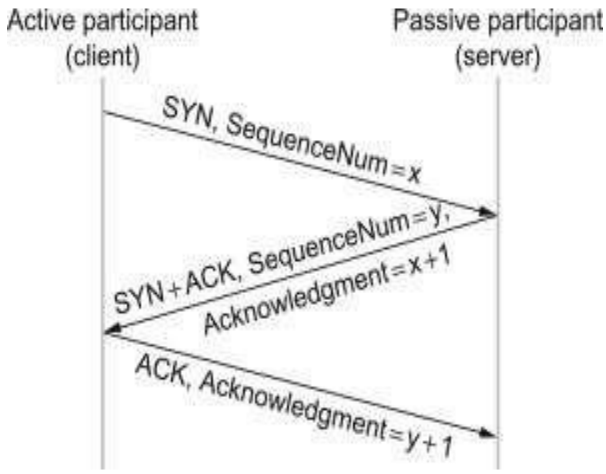
Characteristics	TCP	UDP
Connection	TCP is connection oriented Protocol	UDP is connection less Protocol
Reliability	It provides reliable Delivery of messages	It provides unreliable delivery of messages
Error Handling	TCP makes checks For errors and reporting	UDP does error checking but no reporting.
Flow controlling	TCP has flow control	UDP has no flow control
Data transmission order	TCP gives guarantee that the order of the data at the receiving end is the same as the sending end	No guarantee of the data transmission order
Header Size	20 bytes	8 bytes
Acknowledgment	TCP Acknowledges the data reception	UDP has no acknowledgment Section
Use	Used where reliability is important	Used where time Sensitivity is more important.
Data Interface to application	Stream-based: No particular structure for data	Message based data: Data sent in discrete packages by application
Overhead	Low	Very low
Speed	High	Very high
Application	FTP, Telnet, SMTP, DNS, HTTP, POP	DNS, BOOTP, DHCP, TFTP, RIP

	e	**Compare POP3 with IMAD on below Points.** **i) TCP Port used ii) E-mail Stored at iii) Time required to connect iv) Multiple mail boxes.**	**4 M**
	Ans	**ider the term IMAD as an IMAP**	Each correct Point 1 M Note: Consider the term IMAD as an IMAP

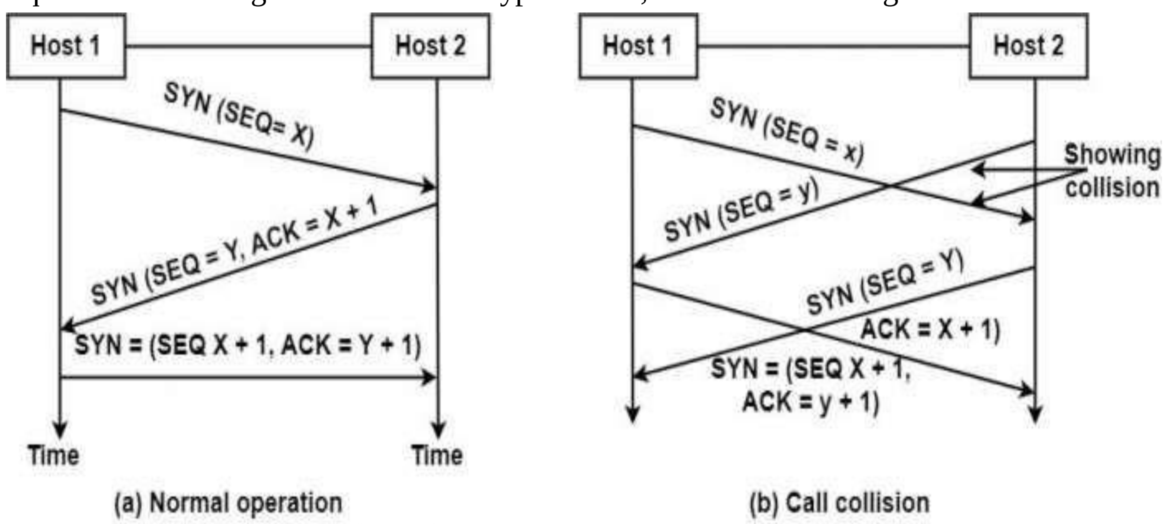
Points	**POP3**	**IMAP**
TCP Port used	Uses port 110 (unencrypted) or port 995 (encrypted/SSL)	Uses port 143 (unencrypted) or port 993 (encrypted/SSL)
E-mail Stored at	Emails are typically downloaded from the server to the client device. The emails are then stored locally on the device, and the server copy is usually deleted.	Emails are stored on the mail server. The client accesses and manages emails directly on the server, allowing for synchronization across multiple devices.
Time required to connect	Generally faster to connect because it involves downloading emails to the client device. Connection time is minimal since it retrieves emails and disconnects from the server.	May take more time to connect as it involves syncing with the server and fetching email headers. However, subsequent access to emails is faster as only headers are initially downloaded.
Multiple mail boxes.	Usually does not support multiple mailboxes. Emails are typically downloaded to a single device, and managing emails on multiple devices can be challenging.	Supports multiple mailboxes and folders Changes made on one device (e.g., marking an email as read) are reflected on all devices since the emails are stored centrally on the server.

5		**Attempt any TWO of the following:**	**12 M**
	a	**Explain how TCP connections are established using 3 way handshake.**	**6 M**

	Ans	**TCP Connection:** When you establish a new TCP connection (3-way handshake) then the initial sequence number is a random 32-bit value. The receiver will use this sequence number and sends back an acknowledgment. Protocol analyzers like wireshark will often use a relative sequence number of 0 since it's easier to read than some high random number. TCP uses a three-way handshake to establish a reliable connection. The connection is full duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other. The exchange of these four flags is performed in three steps: SYN, SYN-ACK, ACK, as shown in figure below  The client chooses an initial sequence number, set in the first SYN packet. The server also chooses its own initial sequence number, set in the SYN/ACK packet. Each side acknowledges each other's sequence number by incrementing it: this is the acknowledgement number. The use of sequence and acknowledgement numbers allows both sides to detect missing or out-of-order segments. Once a connection is established, ACKs typically follow for each segment. The connection will eventually end with a RST (reset or tear down the connection) or FIN (gracefully end the connection). **Three-Way Handshake:** The algorithm used by TCP to establish and terminate a connection is called a three-way handshake. We first describe the basic algorithm and then show how it is used by TCP.	2M for diagram, 1 M for TCP Connection and 3M for 3-way handshake explanation

		The three-way handshake involves the exchange of three messages between the client and the server, as we see in below figure 	
	b	**Demonstrate with suitable example of call collision in TCP connection.**	**6 M**

Ans The connection is established in TCP using the three-way handshake as discussed earlier to create a connection. One side, say the server, passively stays for an incoming link by implementing the LISTEN and ACCEPT primitives, either determining a particular other side or nobody in particular. The other side performs a connect primitive specifying the I/O port to which it wants to join. The maximum TCP segment size available, other options are optionally like some private data (example password). The CONNECT primitive transmits a TCP segment with the SYN bit on and the ACK bit off and waits for a response. The sequence of TCP segments sent in the typical case, as shown in the figure below –



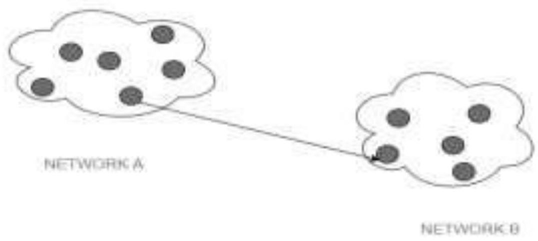
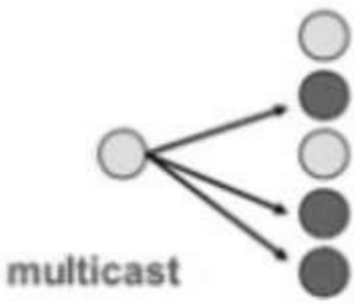
TCP Connection Management

When the segment sent by Host-1 reaches the destination, i.e., host -2, the receiving server checks to see if there is a process that has done a LISTEN on the port given in the destination port field. If not, it sends a response with the RST bit on to refuse the connection. Otherwise, it governs the TCP segment to the listing process, which can accept or decline (for example, if it does not look similar to the client) the connection.

Call Collision: If two hosts try to establish a connection simultaneously between the same two sockets, then the events sequence is demonstrated in the figure under such circumstances. Only one connection is established. It cannot select both the links because their endpoints identify connections.

1 M for diagram, 2 M for TCP connection And 3M for call collision

		Suppose the first set up results in a connection identified by (x, y) and the second connection are also released up. In that case, only tail enter will be made, i.e., for (x, y) for the initial sequence number, a clock-based scheme is used, with a clock pulse coming after every 4 microseconds. For ensuring additional safety when a host crashes, it may not reboot for sec, which is the maximum packet lifetime. This is to make sure that no packets from previous connections are roaming around.	
	c	**Explain following address types of IPv6:** **a) Unicast address** **b) Multicast address** **c) Anycast address**	**6 M**

	Ans	The three types of IPv6 addresses are: unicast, anycast, and multicast. **a) Unicast address:** This type of information transfer is useful when there is a participation of single sender and single recipient. So, in short you can term it as a one-to-one transmission. For example, a device having IP address 10.1.2.0 in a network wants to send the traffic stream (data packets) to the device with IP address 20.12.4.2 in the other network, then unicast comes into picture. This is the most common form of data transfer over the networks.  UNICAST EXAMPLE **b) Multicast address:** In multicasting, one/more senders and one/more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets server's direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols like IGMP (Internet Group Management Protocol), Multicast routing for its working. Also, in Classful IP addressing Class D is reserved for multicast groups.  **c) Anycast address**: An IPv6 anycast address is an address that is assigned to more than one interface (typically belonging to different nodes), where a packet sent to an anycast address is routed to the nearest interface having that address, according to the	2 M for each address types

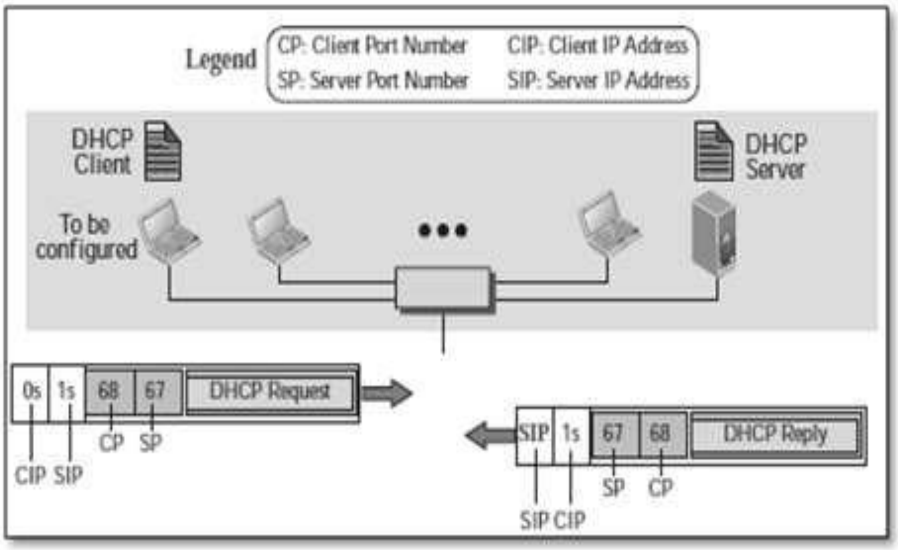
		routing protocol's measure of distance. Anycast addresses, when used as part of a route sequence, permit a node to select which of several Internet service providers it	

		wants to carry its traffic. This capability is sometimes called source selected policies. You implement this by configuring anycast addresses to identify the set of routers belonging to Internet service providers (for example, one anycast address per Internet service provider). You can use these anycast addresses as intermediate addresses in an IPv6 routing header, to cause a packet to be delivered by a particular provider or sequence of providers. You can also use anycast addresses to identify the set of routers attached to a particular subnet or the set of routers providing entry into a particular routing domain. You can locate anycast addresses from the unicast address space by using any of the defined unicast address formats. Thus, anycast addresses are syntactically indistinguishable from unicast addresses. When you assign a unicast address to more than one interface, that is, turning it into an anycast address, you must explicitly configure the nodes to which the address is assigned in order to know that it is an anycast address.	
6		**Attempt any TWO of the following:**	**12 M**
	a	**Explain Distance vector routing and open shortest path first routing protocol in detail.**	**6 M**

	Ans	**1. Distance Vector Routing Protocol:** A distance-vector routing protocol in data networks determines the best route for data packets based on distance. Distance-vector routing protocols measure the distance by the number of routers a packet has to pass, one router counts as one hop. Some distance-vector protocols also take into account network latency and other factors that influence traffic on a given route. To determine the best route across a network, routers, on which a distance-vector protocol is implemented, exchange information with one another, usually routing tables plus hop counts for destination networks and possibly other traffic information. Distance-vector routing protocols also require that a router informs its neighbours of network topology changes periodically. **Distance Vector Algorithm –** • A router transmits its distance vector to each of its neighbours in a routing packet. • Each router receives and saves the most recently received distance vector from each of its neighbours. • A router recalculates its distance vector when: • It receives a distance vector from a neighbour containing different information than before. • It discovers that a link to a neighbour has gone down. **2. Open Shortest Path First (OSPF) Protocol:** The OSPF (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network. The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbours. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.	3 M for each Protocol

		Each OSPF router distributes information about its local state (usable interfaces and reachable neighbors, and the cost of using each interface) to other routers using a Link State Advertisement (LSA) message. Each router uses the received messages to build up an identical database that describes the topology of the AS. From this database, each router calculates its own routing table using a Shortest Path First (SPF) or Dijkstra algorithm. This routing table contains all the destinations the routing protocol knows about, associated with a next hop IP address and outgoing interface. The protocol recalculates routes when network topology changes, using the Dijkstra algorithm, and minimizes the routing protocol traffic that it generates. It provides support for multiple paths of equal cost. It provides a multi-level hierarchy (two-level for OSPF) called "area routing," so that information about the topology within a defined area of the AS is hidden from routers outside this area. This enables an additional level of routing protection and a reduction in routing protocol traffic. All protocol exchanges can be authenticated so that only trusted routers can join in the routing exchanges for the AS.	
	b	**For the IP address given below:** **1) Identify the classes to which IP address belongs to** **2) Identify Network address section** **3) Identify Host address section** **4) Calculate number of hosts can be assigned with each network i)122.34.45.133 ii)12.12.12.12 iii)192.10.233.26**	**6 M**

	Ans	**1.Identify the classes to which IP address belongs to** i)122.34.45.133 = Class A ii)12.12.12.12 = Class A iii)192.10.233.26 = Class C **2. Identify Network address section** i)122.34.45.133 = 122.0.0.0 ii)12.12.12.12 = 12.0.0.0 iii)192.10.233.26 = 192.10.233.0 **3. Identify Host address section** i)122.34.45.133 = 0.34.45.133 ii)12.12.12.12 = 0.12.12.12 iii)192.10.233.26 = 0.0.0.26 **4. Calculate number of hosts can be assigned with each network** i)122.34.45.133 = 232-28=224 ii)12.12.12.12 = 232-28=224 iii)192.10.233.26 = 232-224=28	½ M for identifying each correct class, ½ M for identifying each correct network address section, ½ M for identifying each correct host address section and ½ M for calculating number of hosts
	c	**Describe DHCP operations, when DHCP client and server on same network.**	**6 M**

	Ans	DHCP is based on a client-server model and based on discovery, offer, request, and ACK.DHCP client and server can either be on the same network or on different networks. DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP. DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices. DHCP can be implemented on small local networks, as well as large enterprise networks. DHCP assigns new IP addresses in each location when devices are moved from place to place, which means network administrators do not have to manually configure each device with a valid IP address or reconfigure the device with a new IP address if it moves to a new location on the network.  In this case, the operation can be described as follows: 1. The DHCP server issues a passive open command on UDP port number 67 and waits for a client. 2. A booted client issues an active open command on port number 68. The message is encapsulated in a UDP user datagram, using the destination port number 67 and the source port number 68. 3. The server responds with either a broadcast or a unicast message using UDP source port number 67 and destination port number 68.	2 M for diagram and 4 M for Explanation

MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code : 22520**

Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills.

Q. No	Sub Q.N.	Answer	Marking Scheme

1.		**Attempt any FIVE of the following:**	**10**
	a) **Ans.**	**1. Define Home Agent and Foreign agent with respect to mobile IP.** **Home Agent (HA): -** It is a router on the home network serving as the anchor point for communication with mobile nodes. It tunnels packet from a device on internet, called a correspondent node to a roaming mobile node. **Foreign Agent (FA): -** It is a router that may function as the point of attachment for MN when it roams to a foreign network delivering packets from the Home agent to mobile nodes.	**2M** ***1m for each definitioncorrect***

4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for anyequivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.
8) As per the policy decision of Maharashtra State Government, teaching in English/Marathi and Bilingual (English + Marathi) medium is introduced at first year of AICTE diploma Programme from academic year 2021-2022. Hence if the students in first year (first and second semesters) write answers in Marathi or bilingual language (English +Marathi), the Examiner shall consider the same and assess the answer based on matching of concepts with model answer.

	b) Ans.	**State the need of IPV6 .** **Importance of IPV6 over IPV4 (any two)** **i) huge number of IP addresses:** IPv6 has 128-bit addresses when compared to 32-bit addresses of IPv4 which results in a very large increase in the availability of IP addresses and creates a lot of advantages. **ii) End to End Connectivity:** IPv6 eliminates the need for NAT which results in better connectivit in peer-peer networks. **iii) Interoperability:** IPv6 promotes interoperability between different IPv6 implementations. **iv) Built-in Security:** IPv6 provides authentication and encryption.	**2M** *Any two points 1M each for relevant contents*
	c) Ans.	**1. Distinguish between FTP & TFTP protocols.**	**2M** *Any two points 1M each for relevant contents*

2. FTP	TFTP
File Transfer Protocol	Trivial File Transfer Protocol
It uses 2 connections	It uses 5 connections
Provides many commands	Provides only 5 commands
Uses TCP	Uses UDP
Client must login to the server	No login procedure

Allow for user authentication	Dosen't allow for user authentication
It is reliable	It is unreliable

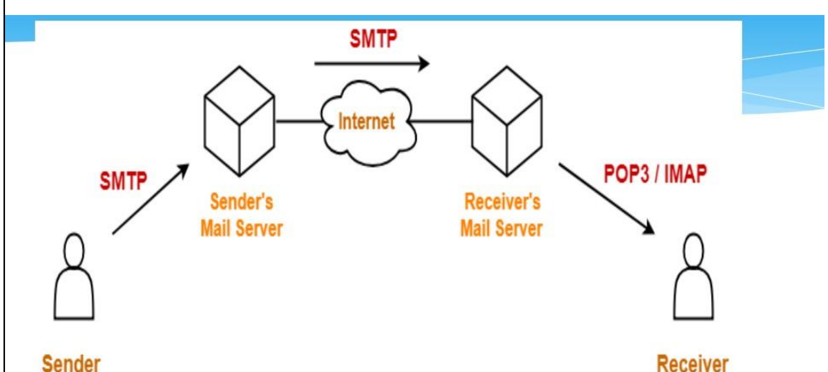
	d) **Ans.**	**2. State any four features of TCP.** 1. TCP is connection oriented Protocol. 2. It provides reliable delivery of messages. 3. TCP makes checks for errors and reporting. 4. TCP has flow control. 5. TCP has High Speed.	**2M** ***four points 1/2M each for relevant contents***
	e) **Ans.**	**Define inter-domain routing protocol. List them.** Routing between autonomous system is referred to as interdomain routing Types – Path Vector (BGP).	**2M** ***Correct explanation 2M***

	f) **Ans.**	**State different applications of UDP.** **Lossless data transmission** UDP can be used in applications that require lossless data transmission. For example, an application that is configured to manage the process of retransmitting lost packets and correctly arrange received packets might use UDP. This approach can help to improve the data transfer rate of large files compared to TCP. **Gaming, voice and video** UDP is an ideal protocol for network applications in which perceived latency is critical, such as in gaming, voice and video communications. **Services that don't need fixed packet transmission** UDP can also be used for applications that depend on the reliable exchange of information but should have their own methods to answer packets. **Multicasting and routing update protocols** UDP can also be used for multicasting because it supports packet switching. In addition, UDP is used for some routing update protocols, such as Routing Information Protocol (RIP).	**2M** ***Any two points 1M each for relevant contents***

	g) **Ans.**	**List two protocols of each for connection-oriented service and connection less service.** Connection-Oriented Service = TCP, Telnet, FTP. Connection-less Service = UDP, IP, ICMP.	**2M** ***Any two points 1M each for relevant contents***

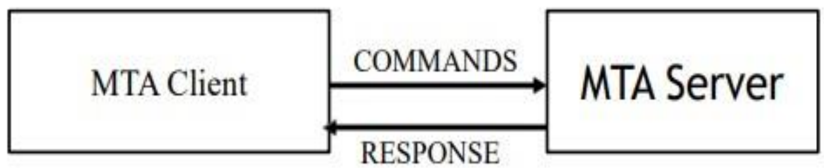
SUMMER – 2023 EXAMINATION

MODEL ANSWER

2.		**Attempt any <u>THREE</u> of the following:**	**12**
	a)	**Describe SMTP with suitable diagram.**	**4M**
	Ans.	It is the protocol that defines MTA client & server in internet. • It is an application layer protocol of TCP/IP model. • It transfer messages from sender's mail servers to receivers mail server. • SMTP interacts with local mail system and not user. • SMTP uses a TCP socket on port 25 to transfer email reliably from client to server. • Email is temporarily stored on the local and eventually transferred directly to receiving server. • It is simple ASCII protocol.  	***Diagram 2M*** ***Explanation 2M***

COMMANDS & RESPONSE

SMTP uses commands and response to transfer message between MTA client and MTA server



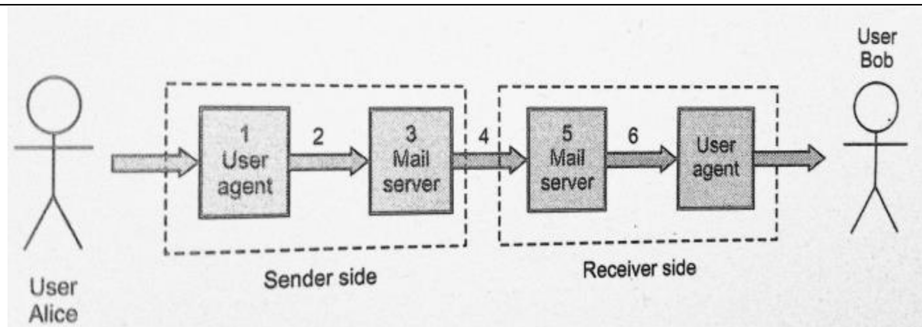
SMTP Commands:

1. HELO: Used by client to identify itself.
2. MAIL FROM: Identify sender.
3. RCPT TO: Identify intended recipient.
4. DATA: Send actual message.
5. QUIT: Terminate the message.
6. RSET: Reset the connection.
7. VRFY: Verify the add of recipient
8. HELP: Mail

Example: Scenario: Alice sends message to Bob

1. Alice uses user agents (UA) to compose message and send to bob@technical.org.
2. Alice UA sends message to her mail server, message placed in message queue.
3. Client side of SMTP opens TCP connection with Bob's mail server.
4. SMTP client sends Alice message over TCP connection. 5. Bob's mail server places the message in Bob's mailbox.

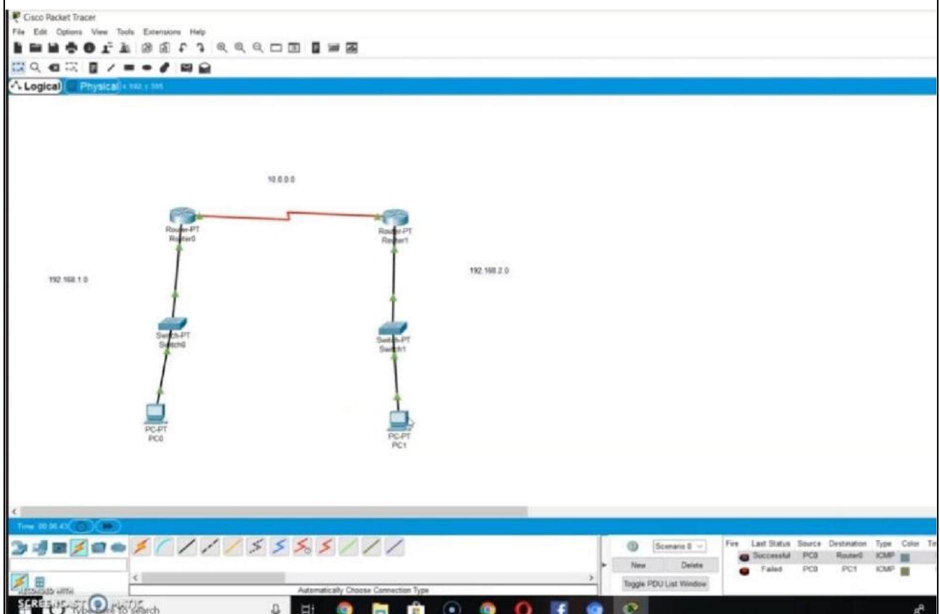
6. Bob invokes his user agent to read message.

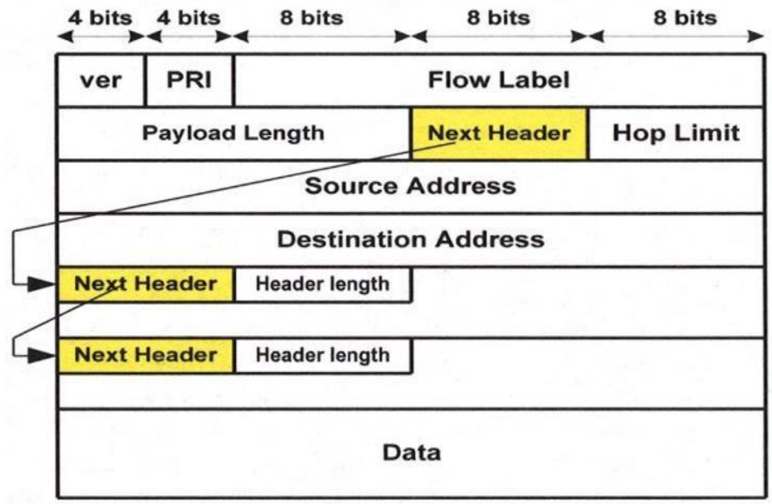

User
Bob
1
User
agent
2
3
Mail
server
4
5
Mail
server
6
User
agent
User
Alice
Sender side
Receiver side

SUMMER – 2022 EXAMINATION MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code : 22520**

	b) Ans.	**Write Stepwise Procedure to configure IP routing with RIP.** • The Routing Information Protocol (RIP) uses broadcast UDP data packets to exchange routing information A device that is running RIP can receive a default network via an update from another device that is running RIP, or the device can source the default network using RIP. • Once you have configured the appropriate IP addresses on each device, perform the following steps to configure RIP routing. The default version of RIP. 1. On Router1, execute the following commands to configure RIP routing. Router1(config)#router rip Router1(config-router)#network 10.0.0.0 Router1(config-router)#network 192.168.1.0 Router1(config-router)#exit 2. On Router2, execute the following commands to configure RIP routing. Router2(config)#router rip Router2(config-router)#network 20.0.0.0 Router2(config-router)#network 192.168.1.0 Router2(config-router)#network 150.150.150.0 Router2(config-router)#exit Router2(config)# 3. On Router3, execute the following commands to configure RIP routing. 4. Router3(config)#router rip 5. Router3(config-router)#network 150.150.150.0 Router3(config-if)#exit 6. Once you have configured RIP routing protocol on each router, wait for a few seconds (let complete the convergence process), and then execute the show ip route command on any router to show the routing information. Router(config)#do show ip route 7. In the following figure, you can see the routes learned by the RIP protocol on Router3.	**4M** **Explanation of steps**

		 Cisco Packet Tracer File Edit Options View Tools Extensions Help Logical Physical 10.0.0.0 192.168.1.0 192.168.2.0	

	c) Ans.	**Draw and explain IPv6 protocol format**  1. Version: This 4 bits field defines the version number of IP. The value is 6 for IPV6. 2. Priority: This 4 bits priority field defines the priority of packet with respect to traffic congestion. 3. Flow Label: It is 24 bits field that is designed to provide special handling for a particular flow of data. 4. Payload Length: The 16 bits payload length field defines the length of the IP datagram excluding the base header.	**4M** *Diagram 2M* *Explanation 2M* *Any other relevant Explanation Shall be considere d*

5. Next Header: It is an 8 bits field defining the header that follows the base header in datagram.
6. Hop Limit: This 8 bits field serves the same purpose as the TTL field in IPV4.
7. Source Address: The source address field is a 128 bits internet address that identifies the original.
8. Destination Address: It is 128 bits internet address that usually identifies the final destination of datagram.
9. Payload: Is combination of zero or more extension headers(options) which is followed by data from other protocols such as UDP, TCP etc

EXTENSION HEADERS

• The length of the base header is fixed at 40 bytes.

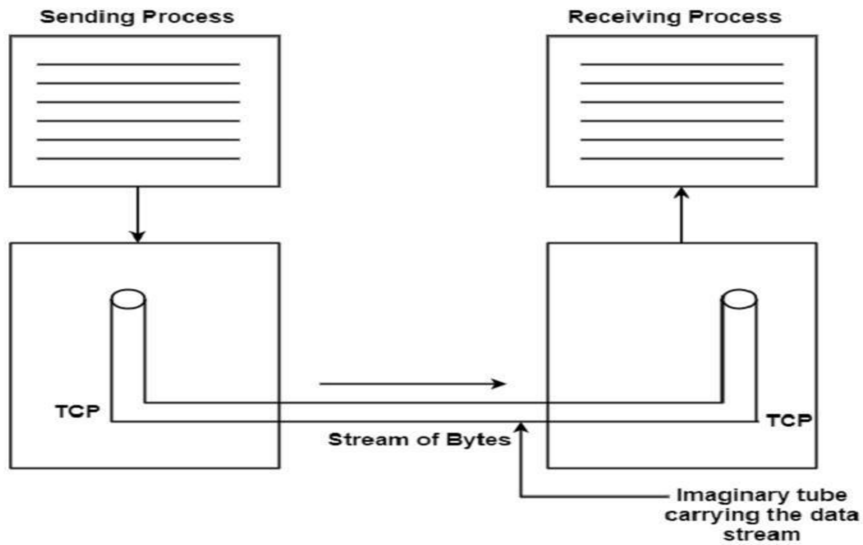
• Types of extension headers are:

1. Hop by Hop option
2. Source routing
3. Fragmentation
4. Authentication
5. Encrypted security payload
6. Destination option

Hop by Hop options is used when the source needs to pass information to all the routers visited by the datagram.

2. Source routing extension header combines the concept of strict source route & the loose source route options of IPV4.
3. Fragmentation is the same as that in IPV4. in IPV6 only the original source can be fragment.

		4. Authentication header has a dual purposes: it validates the message sender & ensure the integrity of data. 5. Encrypted security Payload is an extension that provides confidentiality & guards. 6. Destination option is used when the service needs to pass information to destination only, intermediate routers are not permitted access to this information.	

	d) Ans.	**List and explain ,services provided by TCP** Transmission Control Protocol (TCP) to the processes at the application layer: • Stream Delivery Service. • Full Duplex Service • Connection Oriented Service. • Reliable Service. **Stream Delivery Service** TCP is a stream-oriented protocol. It enables the sending process to deliver dataas a stream of bytes and the receiving process to acquire data as a stream of bytes. TCP creates a working environment so that the sending and receiving procedures are connected by an imaginary "tube", as shown in the figure below:  	**4M** *List 1M Explanation 3M For relevant Contents.*

Full-Duplex Service

TCP offers a full-duplex service where the data can flow in both directions simultaneously. Each TCP will then have a sending buffer and receiving buffer. The TCP segments are sent in both directions.

Connection-Oriented Service

We are already aware that the TCP is a connection-oriented protocol. When a process wants to communicate (send and receive) with another process (process -2), the sequence of operations is as follows:

- TCP of process-1 informs TCP of process-2 and gets its approval. • TCP of process-1 tells TCP of process-2 exchange data in both directions.
- After completing the data exchange, when buffers on both sides are empty, the two TCPs destroy their buffers.

The type of connection in TCP is not physical, but it is virtual. The TCP segment encapsulated in an IP datagram can be sent out of order. These segments can get lost or corrupted and may have to be resend. Each segment may take a different path to reach the destination

Reliable Servic

TCP is a reliable transport protocol. It uses an acknowledgment mechanism for checking the safe and sound arrival of data.

3.		**Attempt any THREE of the following:**	**12**
	a)	**Distinguish between dynamic routing and static routing on the basis of configuration ,security, routing protocols and cost.** .	**4M**
	Ans.		*1M for any 4 points*

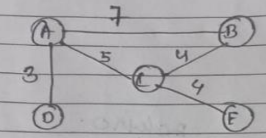
Basis of comparison	**Static Routing**	**Dynamic Routing**
Configuration	Manually done	Automatically done
Routers	Routing location by hand typed	Dynamically fill all locations
Routing algorithms	Does not support complex algorithm	Supports more complex algorithm for routing purposes
Used in	In small networks	In large networks
Filure of links	Link failure disturb rerouting	Link failure doesnot disturb the rerouting
Security	More secure because no advertisement send with data	Less secure because sending multicast and broadcasts
Routing Protocol	No routing protocols are added in the routing process	Routing protocols such as RIP EIGRP etc are included in all routing process
Extra resources	There is no extra resource like memory and CPU.	It requires resource like memory and CPU etc.

	b)	**For the IPV4 addresses given below, calculate subnet mark, broadcast addresses and number of host possible.** **i) 10.0.199.237/22** **ii)192.168.14.87/26**	

	Ans	. **i. 10.0.199.237/22** Subnet Mask 255.255.252.0 Network Address 10.0.199.237= 00001010.00000000.11000111.11101101 AND 255.255.252.0=11111111.11111111.11111100.00000000 --- 10.0.196.0 =00001010.00000000. 11000100.00000000 No of host 2^{10}-2=1022 Broadcast Address 10.0.199.255 Range IP Address 10.0.196.1 - 10.0.199.254 **ii. 192.168.14.87/26** Subnet Mask 255.255.255.192 Network Address 192.168.14.87= 11000000.10101000. 00001110.01010111 AND 255.255.255.192=11111111.11111111.11111111.11000000 --- 192.168.14.64 =11000000. 10101000. 00001110.01000000 No of host 2^{6} -2=62 Broadcast Address 192.168.14.127 Range Of IP 192.168.14.65 - 192.168.14.126	**4M** ***2M for each Calculation***

	c)	**Differentiate between IPv4 and IPv6 (any 4 points)**	**4M**
	Ans.	(table below)	*Any 4 points* *IM each*

Sr. No.	IPv4	IPv6
1	IPv4 addresses are 32 bits i.e. 4 bytes length	IPv6 addresses are 128 bits i.e. 16 bytes length
2	Header length is 20 bytes	Header length is 40 bytes
3	Checksum is available in header	No Checksum in header
4	IPv4 allows 5 different classes of IP address	IPv6 allows storing an unlimited of IP address
5	No packet flow identification	Packet flow identification is available
6	Limited addresses	Larger address space

	d)	**Use Bellman – Fort algorithm to find the shortest distance for all**	**4M**
	Ans	S-22 Q3. d. 	***1M each for each iteration***

Source vertex = A

Edge	weight
A – B	7
A – C	5
A – D	3
B – C	4
C – E	4

formula: $v.d > u.d + w(u,v)$

$v.d = u.d + w(u.v)$

where
u = start vertex
v = End vertex
w(u,v) = weight of (u,v).

		nodes in the graphs	

MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code : 22520**

It.1

	A	B	C	D	E
d	0	7	∞	∞	∞
	0	7	5	∞	∞
	0	7	5	3	∞
	0	7	5	3	∞
	0	7	5	3	9

It.2.

	A	B	C	D	E
d	0	7	5	3	9
	0	7	5	3	9
	0	7	5	3	9
	0	7	5	3	9
	0	7	5	3	9

It.3

	A	B	C	D	E
d	0	7	5	3	9
	0	7	5	3	9
	0	7	5	3	9
	0	7	5	3	9
	0	7	5	3	9

It-4

	A	B	C	D	E
d	0	7	5	3	9
	0	7	5	3	9
	0	7	5	3	9
	0	7	5	3	9
	0	7	5	3	9

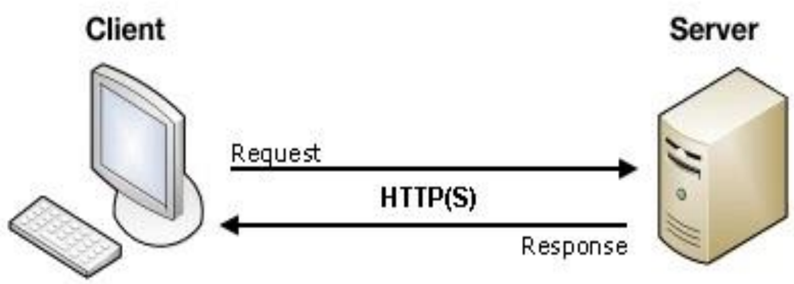
Subject: Advanced Computer Network (Elect) **Subject Code : 22520**

4.		**Attempt any THREE of the following:**	**12**
	a)	**Define WWW. Explain static & dynamic web documents in details.**	**4M**
	Ans	**World Wide Web(WWW):** • WWW is a collection of millions of files stored on thousands of servers all over the world. • Those files represent documents, pictures, videos, sounds, programs etc. **Web Browsers-** • A web browser is a program. • Is used to communicate with web server on the internet, which enables it to download and display the webpages. • Netscape Navigate & Microsoft internet explorer are the most popular browsers. **Working of Browsers-** • WWW works on client-server interaction. • The browser program acts as a client that uses the internet to contact a remote server for a copy of the requested page. • The server on the remote system returns a copy of page along with the additional information. **Following steps explain how web works:** 1. User enters the URL (say https:// www.google.com of the web page in address bar of web browsers. 2. Then browser request the Domain Name server for IP address corresponding to www.google.com. 3. After receiving IP address, browsers sends the request for webpage to web server using HTTP protocol which specifies the way the browser and web server communicates.	***Diagram 2M*** ***Explainati on 2M***

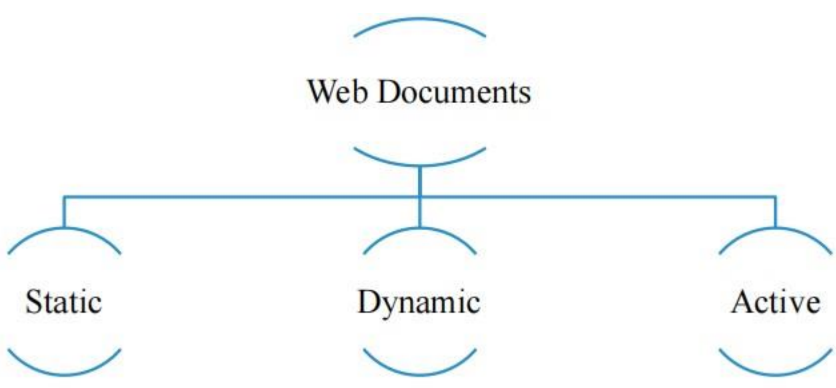
		4. Then web server receives request using HTTP protocol and check it search for the requested webpage. If found it returns back to the web browsers and close the HTTP connection. 5. Now, the web browser receives the web page, it interprets it and display the contents of web page in web browser's windows.	

SUMMER – 2023 EXAMINATION

MODEL ANSWER

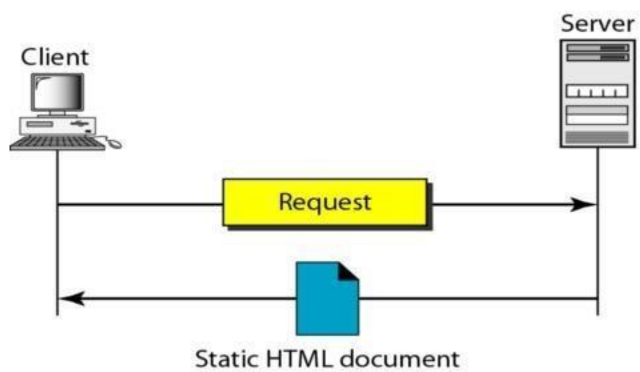


Web Documents-



1. STATIC DOCUMENTS-

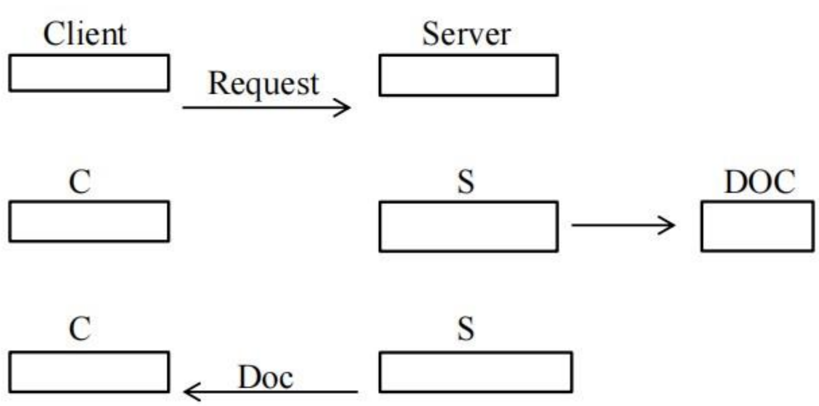
- The contents of static documents are fixed. These contents are created and stored in a server.
- If required the client can get a copy of static documents.

		• The contents of static documents are determined when it is created. 	

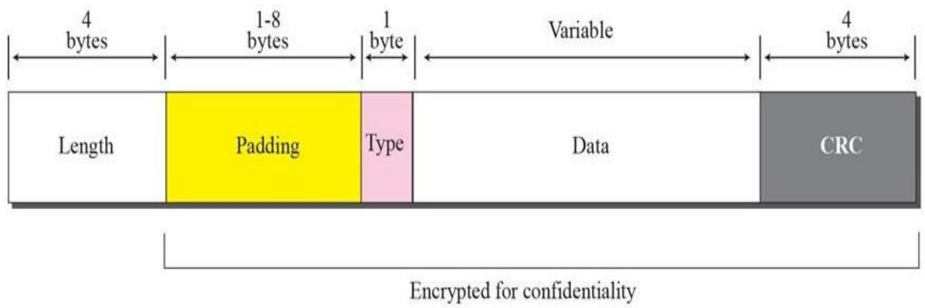
2. DYNAMIC DOCUMENT-

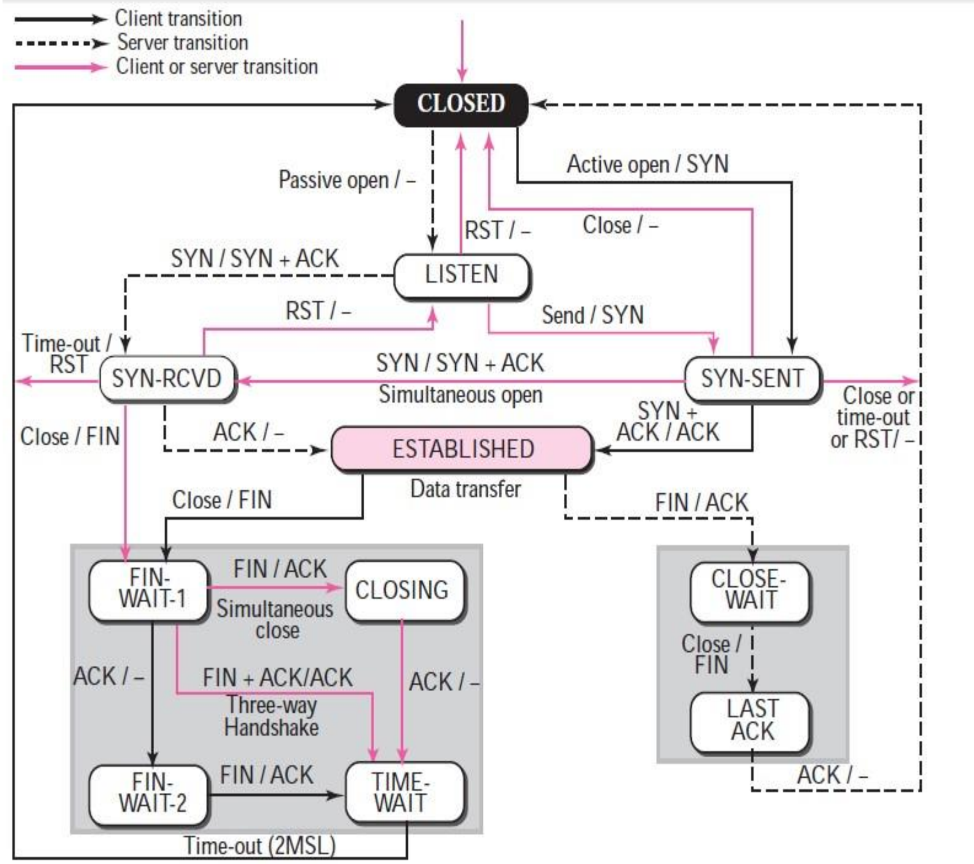
- It is not defined in a pre-define format, like static documents.
- It is created by a web browser on the request for the document from a browser.

•

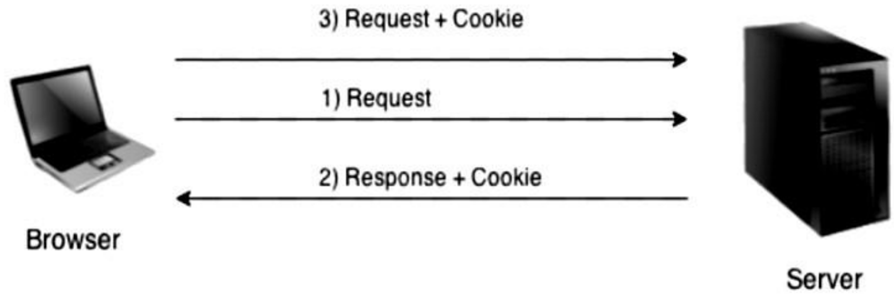


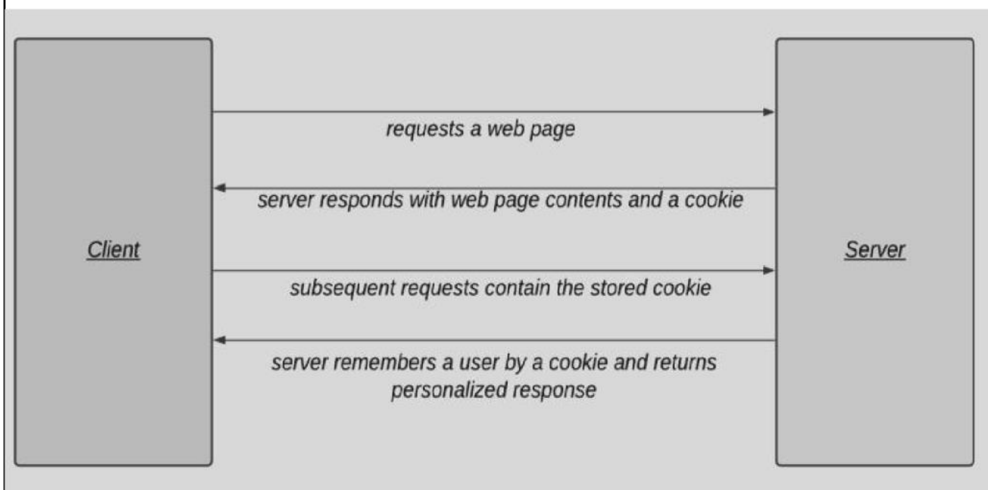
1. Client sends request.
2. Server runs a program create a dynamic doc.
3. Server sends the doc to client.

	b) **Ans**	**Explain the frame format of SSH** SSH *Format-* **1. Length:** It indicates the size of the packet, not including the length field or the variable length random padding fields that follows it.  **2. Padding:** It causes an intrusion to be more difficult. **3. Type:** It identifies the type of message. **4. CRC:** It is an error detection field.	**4M** ***Diagram 2M*** ***Explainati on 2M***

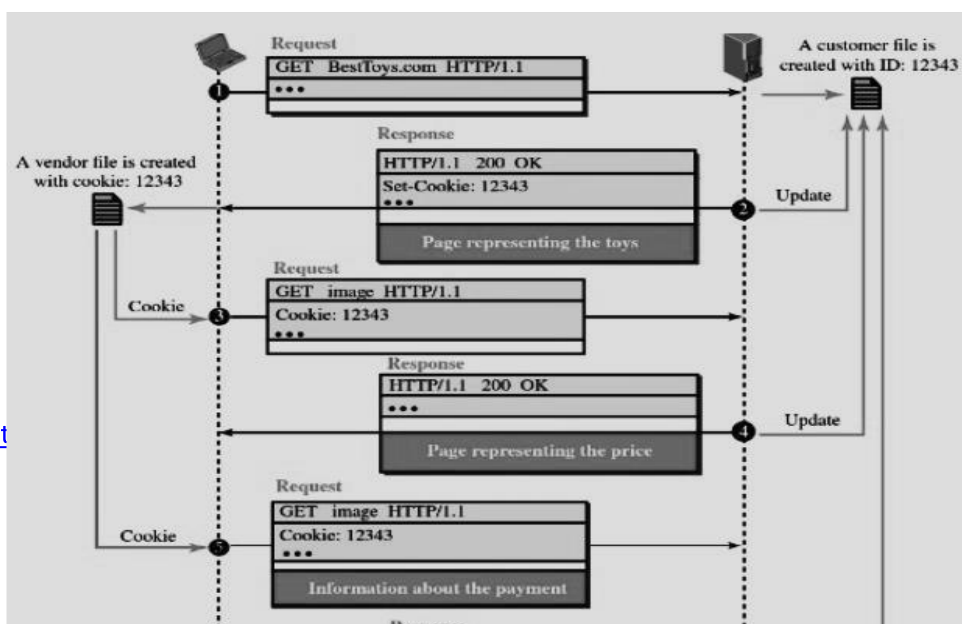
	c) Ans.	**Draw state transition diagram of TCP.** 	**4M** *4M for Diagram & labelling*

	d) Ans	**Explain functioning of multicast link. State routing protocol. DVMRP- Distance Vector Multicast Routing Protocol:** • Is an internet routing protocol that provides an efficient mechanism for connection-less datagram delivery to a group of hosts across an internetwork. • It is a distributed protocol that dynamically generate IP multicast delivery tress using a technique called reverse path multicasting. • DVMRP uses a distance vector distributed routing algorithm in order to build per-source-group multicast delivery tree. • Each router maintains a multicast routing table by exchanging distance vector information among. • It constructs a source tree for each group using reverse path forwarding. • Multiple routers on the same/AN select designated forwarder by lower metric or lower IPaddress. • Once a tree is created, it is used to forward message from source to receivers. • Flood multicast packets based on reverse path forwarding rule to all routers. • Upstream router prunes the interface with no dependent downstream router.	***4M*** ***4M for Explaining***

	e)	**Construct a diagram to show the application of cookies in a scenario in which the server uses cookies for advertisement.**	***4M***
	Ans	Cookies are small files which are stored on a user's computer. They are used to hold a modest amount of data specific to a particular client and website and can be accessed either by the web server or by the client computer.  When cookies were invented, they were basically little documents containing information about you and your preferences. For instance, when you select your language in which you want to view your website, the website would save the information in a document called a cookie on your computer, and the next time when you visit the website, it would be able to read a cookie saved earlier. That way the website could remember your language and let you view the website in your preferred language without having to select the language again. A cookie can contain any type of information such as the time when you visited the website, the items that you added into your shopping basket, all the links you clicked in website, etc. Cookies themselves contain no personally identifiable information. Depending on the publisher's and the user's settings, information associated with cookies used in advertising may be added to the user's Google Account.	***2M for Explanation & 2M for Diagram***



Most commonly, AdSense sends a cookie to the browser when a user visits a page that shows Google ads. Pages with Google ads include ad tags that instruct browsers to request ad content from our servers. When the server delivers the ad content, it also sends a cookie. But a page doesn't have to show Google ads for this to happen; it just needs to include our ad tags, which might load a click tracker or impression pixel instead. Following Fig. Example of how server uses cookies for advertisement.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

SUMMER _ 2023 EXAMINATION

MODEL ANSWER

SUMMER – 2022 EXAMINATION MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code : 22520**

5.		**Attempt any TWO of the following:**	**12**
	a)	**Differentiate between TCP, UDP and SCTP on basis of relability, connection management, transmission of message ,flow control ,security and data delivery.**	**6M**
	Ans.	(see table below)	***Each correct difference 1 mark each***

Services/Features	SCTP	TCP	UDP
Full-duplex data transmission	yes	yes	yes
Connection-oriented	yes	yes	no
Reliable data transfer	yes	yes	no
Partially reliable data transfer	optional	no	no
Ordered data delivery	yes	yes	no
Unordered data delivery	yes	no	yes
Flow and congestion control	yes	yes	no
Explicit congestion notification support	yes	yes	no
Selective acks	yes	optional	no
Preservation of message boundaries	yes	no	yes
Path maximum transmission unit discovery	yes	yes	no
Application data fragmentation/bundling	yes	yes	no
Multistreaming	yes	no	no
Multiboming	yes	no	no
C. ction against SYN flooding attack	yes	no	n/a
Half closed connections	no	yes	n/a

	b) **Ans**	**Describe DHCP with its operation & static dynamic allocation.** The Domain Name System, more popular as DNS, and the Dynamic Host Configuration Protocol, also known as DHCP, represent two crucial TCP/IP areas of a Windows NT Server network. The DNS is responsible for converting hostnames into IP addresses, while the DHCP is engaged in assigning unique dynamic IP addresses and the corresponding subnet masks and default gateways to TCP/IP running computers within a particular server network. Thanks to the dynamic addressing executed by the DHCP, a computer can have a different IP address every time it connects to the network it belongs to, without the intervention of a UNIX administrator. Through this DHCP functionality every new computer added to a network is automatically assigned a unique IP address.	

		DHCP servers greatly simplify the configuration of networks and are built in the majority of the wireless access points and wired Ethernet routers. In a network, a DHCP server manages a pool of IP addresses, as well as default gateway details, DNS details and other information for the clients' network configuration. When a new computer is introduced into a DHCP server-enabled network, it will send a query to the DHCP server requesting all the necessary information. When the query reaches the DHCP server, it will grant the new computer a new IP address and a lease - a time frame for which the computer can use this IP address, as well as other configuration details. The whole process takes place immediately after the new computer boots, and to be successful, it has to be completed before initiating IP based communication with other hosts in the network. **STATIC ALLOCATION** The static allocation method is very popular in modern ISP networks, which do not use dial-up methods. With the static allocation, the DHCP sever keeps a database with all clients' LAN MAC addresses and gives them an IP address only if their MAC address is in the database. This way, the clients can be sure that they will be getting the same IP address every time. **DYNAMIC ALLOCATION** When the DHCP server is configured to use dynamic allocation, this means that it uses a lease policy. This way, when an assigned IP address from the available pool is no longer used, it will be transferred back to the pool, making it available for someone else to use. The advantage of this method is that the IP addresses are used to their maximum - as soon as they are no longer used by the client, they are instantly made available to others. The disadvantage of this method is that a client will always have a random IP address.	

	c) Ans	**Describe Email security Over non-secure channel.** • Email security describes different techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss or compromise • Email is often used to spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to part with sensitive information, open attachments or click on hyperlinks that install malware on the victim‟s device. • Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than intended recipients. Email encryption often includes authentication. • Email allows attackers to use it as a way to cause problems in attempt to profit. Whether through spam campaigns, malware and phishing attacks, sophisticated targeted attacks, or business email compromise (BEC), attackers try to take advantage of the lack of security of email to carry out their actions.	*6M* *Any 6 points 1M each*

		• Since most organizations rely on email to do business, attackers exploit email in an attempt to steal sensitive information. • Because email is an open format, it can be viewed by anyone who can intercept it. It can be easily read and the contents of an email by intercepting it. • Email Security Policies can be established by viewing the contents of emails flowing through their email servers. It"s important to understand what is in the entire email in order to act appropriately. After these baseline policies are put into effect, an organization can enact various security policies on those emails. • These email security policies can be as simple as removing all executable content from emails to more in-depth actions, like sending suspicious content to a sandboxing tool for detailed analysis. • If security incidents are detected by these policies, the organization needs to have actionable intelligence about the scope of the attack. • Enforce email encryption policies to prevent sensitive email information from falling into the wrong hands. • An email gateway scans and processes all incoming and outgoing email and makes sure that threats are not allowed in. Because attacks are increasingly sophisticated, standard security measures, such as blocking known bad file attachments, are no longer effective.	

6.		**Attempt any <u>TWO</u> of the following:**	***6M***
	a) **Ans**	**Explain the process of transition from IPv4 to IPv6 for a network.** Three Transitions from IPv4 to IPv6 strategies are: 1. Dual Stack 2. Tunnelling 3. Header Translation 1**. Dual Stack** In this kind of strategy, a station has a dual stack of protocols run IPv4 and IPv6 simultaneously. To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.	***2M for each transition***

2**. Tunnelling**

Tunnelling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4.

- To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region.
- To make it clear that the IPv4 packet is carrying an IPv6 packet as data.

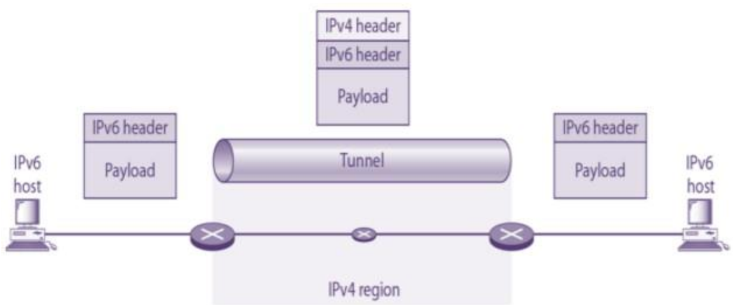


Fig. Tunnelling

3**.Header Translation**

In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header see figure.

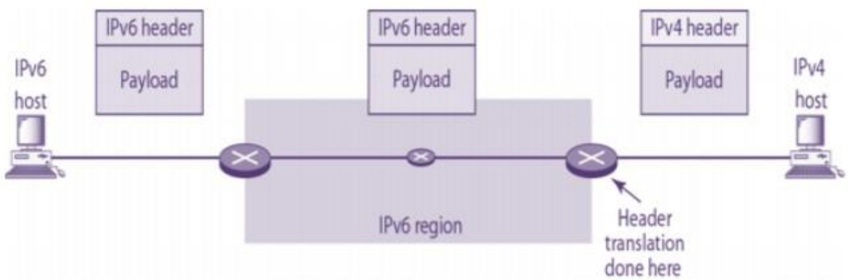
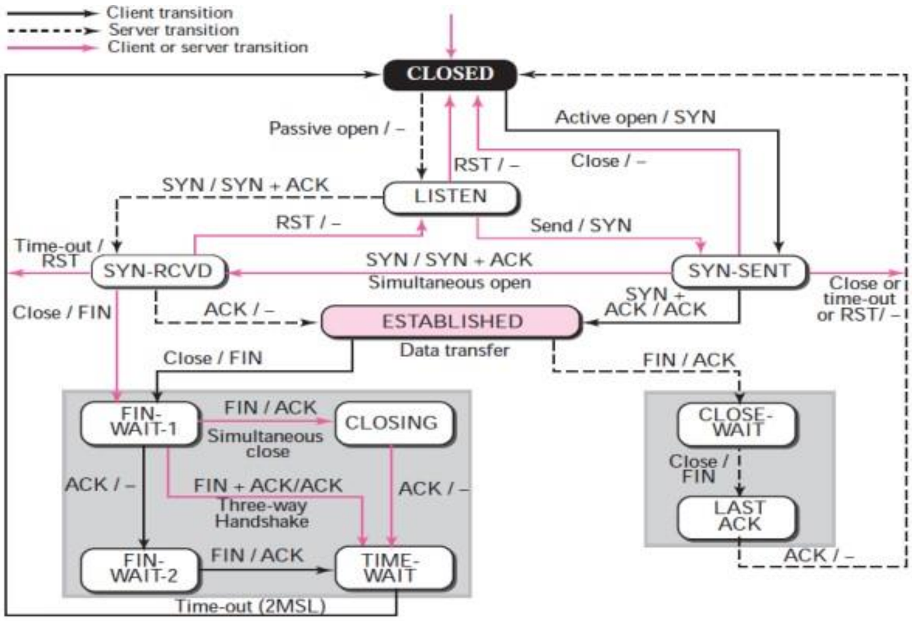


Fig. Header Translation

SUMMER – 2022 EXAMINATION MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code : 22520**

	b) **Ans**	Draw and explain TCP. State transition diagram.	**6M** *3M for diagram & 3M for Explanation*



To keep track of all the different events happening during connection establishment, connection termination, and data transfer, TCP is specified as the Finite State Machine –FSM TCP State Machine:

- TCP uses a three way handshake to close connection.
- Singled by the FIN bit in the packet header The figure shows the two FSMs used by the TCP client and server combined in one diagram.
- Ovals/rectangle represents states.
- Transition from one state to another is shown using directed lines.
- Each line has two strings separated by a slash.
- The first string is the input, what TCP receives.
- The second is the output, what TCP sends.

		• The dotted black lines in the figure represent the transition that a server normally goes through. • The solid black lines show the transitions that a client normally goes through.	

• Sometimes in some situations, a server transitions through a solid line or a client transition through a dotted line.

State	Description
CLOSED	No connection exists
LISTEN	Passive open received; waiting for SYN
SYN-SENT	SYN sent; waiting for ACK
SYN-RCVD	SYN+ACK sent; waiting for ACK
ESTABLISHED	Connection established; data transfer in progress
FIN-WAIT-1	First FIN sent; waiting for ACK
FIN-WAIT-2	ACK to first FIN received; waiting for second FIN
CLOSE-WAIT	First FIN received, ACK sent; waiting for application to close
TIME-WAIT	Second FIN received, ACK sent; waiting for 2MSL time-out
LAST-ACK	Second FIN sent; waiting for ACK
CLOSING	Both sides decided to close simultaneously

	c)	**For the IP address given below:** **i. 132.34.45.133** **ii. 14.142.20.20 iii. 191.0.200.45** **iv. 129.16.123.85** **A. Identify the classes to which the following IP numbers belong to.** **B. Identify the network address section.** **C. Identify host address section.**	*6M* *2M for each question (1/2M for each subquestion)*
	Ans	A) i. 132.34.45.133 : This IP address belongs to Class B. ii. 14.142.20.20 : This IP address belongs to Class A. iii. 191.0.200.45 : This IP address belongs to Class B. iv. 129.16.123.85 : This IP address belongs to Class B.	

		B) In each IP address, the network address section is determined by the class of the IP address. i. 132.34.45.133 Network address: 132.34 ii. 14.142.20.20 Network address: 14 iii. 191.0.200.45 Network address: 191.0 iv. 129.16.123.85 Network address: 129.16 C) The host address section in each IP address is the part remaining after identifying the network address. i. 132.34.45.133 Host address: 45.133 ii. 14.142.20.20 Host address: 142.20.20 iii. 191.0.200.45 Host address: 200.45 iv. 129.16.123.85 Host address: 123.85	

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

SUMMER – 2023 EXAMINATION MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills).

Q. No.	Sub Q.N.	Answer	Marking Scheme
1.		**Attempt any FIVE of the following:**	**10**
	(a) Ans.	**Differentiate between IPv4 and IPv6. (any two)**	**2M**

Sr. No.	**IPv4**	**IPv6**
1	IPv4 addresses are 32 bits i.e. 4 bytes length	IPv6 addresses are 128 bits i.e. 16 bytes length
2	Header length is 20 bytes	Header length is 40 bytes
3	Checksum is available in header	No Checksum in header
4	IPv4 allows 5 different classes of IP address	IPv6 allows storing an unlimited of IP address
5	No packet flow identification	Packet flow identification is available
6	Limited addresses	Larger address space

Any two points 1M each

	(b) Ans.	**State the four advantages of IPv6.**	**2M**

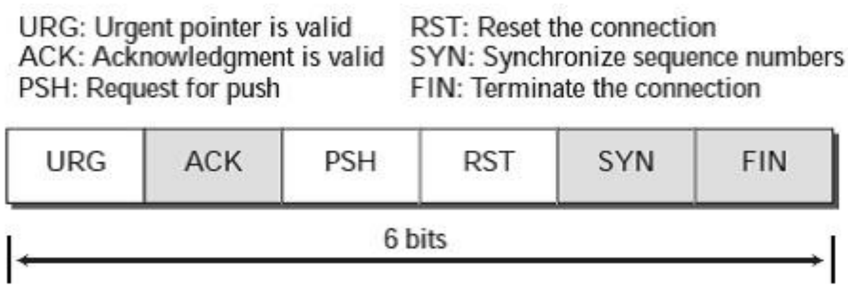
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate‟s answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate‟s understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

		Advantages of IPv6: • Larger address space. • Better header format. • New options for additional functionalities. • Allowance for extension. • Support for more security. • More efficient routing • More efficient packet processing • Directed data flows • Simplified Network configuration • Support for new services • Support for Security • Auto configuration	***Any four advantages ½M each***

<table>
<tr><td></td><td>(c) Ans.</td><td>State the need of domain name system.
Need of domain name system:
• Since IP addresses are difficult to remember and names are easier to remember Domain Name System is used and DNS servers are used for converting these names into IP addresses.
• Large number to hosts and servers connected in the internet can be classified using Domain name system so that hierarchical naming system is implemented.
• To identify an entity, TCP/IP protocols use the IP address. An IP is uniquely identifies the connection of a host to internet. Use for mapping can map a name to an address or an address to a name.</td><td>2M

Any one Need 2M</td></tr>
<tr><td></td><td>(d) Ans.</td><td>State the use of 6 flags in TCP header.
There are 6, 1-bit control bits that control connection establishment, termination, abortion, flow control etc..
<table><tr><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td></tr></table>
1) URG: Urgent pointer
If this bit field is set the receiving TCP should interpret the urgent pointer field.
2) ACK: Acknowledgement
If this bit field is set the ACK field described earlier is valid.
3) PSH: Push function
Request for push
4) RST: Reset the connection
If this bit is present it signals the receiver that sender is aborting the</td><td>2M

Correct use 2M</td></tr>
</table>

		connection i.e. Reset the connection. 5) SYN: Synchronize When this bit field in present then the sender is attempting to „synchronize" sequence numbers 6) FIN: No more data from sender. If this bit is set then it terminates the connection. **OR**  	
	(e) **Ans.**	**List two advantages of using UDP over TCP.** **Advantages of using UDP over TCP:** 1) UDP is connection less and unreliable transport layer protocol. i.e. It does not require to maintain a connection. 2) UDP is transaction oriented and suitable for simple query response protocols. 3) UDP is faster since it does not require acknowledgment. 4) Useful when time sensitivity is more important	**2M** ***Any two advantages 1M each***
	(f) **Ans.**	**State the transmission modes of FTP.** **Transmission modes of FTP:** 1. Stream mode 2. Block mode 3. Compressed mode	**2M** ***Correct modes 2M***

	(g) **Ans.**	**State the concept of fragmentation in IPv4.** Fragmentation: When the maximum size of datagram is greater than maximum size of data that can be held a frame then the network layer divides the datagram received from x-port layer into fragments. OR Fragmentation is the division of a IP datagram into smaller units. After fragmentation, each fragment will have its own header with few fields changed and few fields remaining same. OR	**2M** ***Fragmentation definition 1M***

		In fragmentation, a datagram is divided into smaller units. Most of the fields of the original header are copied into the fragment header. The three fields Flags, Fragmentation offset and Total length are altered.	***Concept 1M***

2.		**Attempt any THREE of the following:**	**12**
	(a)	**Compare TCP and UDP (any four points).**	**4M**
	Ans.		

Characteristics	TCP	UDP
Connection	TCP is connection oriented Protocol	UDP is connection less Protocol
Reliability	It provides reliable delivery of messages	It provides unreliable delivery of messages
Error Handling	TCP makes checks for errors and reporting	UDP does error checking but no reporting.
Flow controlling	TCP has flow control	UDP has no flow control
Data transmission order	TCP gives guarantee that the order of the data at the receiving end is the same as the sending end	No guarantee of the data transmission order
Header Size	20 bytes	8 bytes
Acknowledgment	TCP acknowledges the data reception	UDP has no acknowledgment Section
Use	Used where reliability is important	Used where time sensitivity is more important.
Data Interface to application	Stream-based: No particular structure for data	Message based data: Data sent in discrete packages by application
Overhead	Low	Very low
Speed	High	Very high

Any four points 1M each

Application	FTP, Telnet, SMTP, DNS, HTTP, POP	DNS, BOOTP, DHCP, TFTP, RIP

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

SUMMER – 2023 EXAMINATION

MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

(b) Ans.

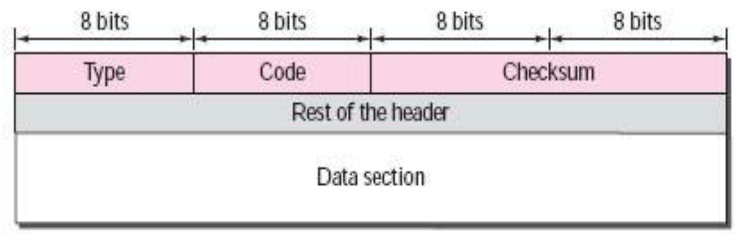
Explain ICMP protocol. Describe the header format of ICMP. The Internet Control Message Protocol (ICMP) supports the unreliable and connectionless Internet Protocol (IP).

4M

- ICMP messages are encapsulated in IP datagrams. There are two categories of ICMP messages: error-reporting and query messages. The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet. The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. □ The checksum for ICMP is calculated using both the header and the data fields of the ICMP message.
- There are several tools that can be used in the Internet for debugging. We can find if a host or router is alive and running. Two of these tools are ping and traceroute.

Explanation 2M

Header Format:



Format 1M

An ICMP message has an 8-byte header and a variable-size data section. Although the general format of the header is different for each message type, the first 4 bytes are common to all. As Figure shows,

- The first field, ICMP type, defines the **type** of the message.
- The **code field** specifies the reason for the particular message type.
- The last common field is the **checksum field** for checking errors □ The rest of the header is specific for each message type.

Description 1M

		• The data section in error messages carries information for finding the original packet that had the error. In query messages, the data section carries extra information based on the type of the query.	

	(c) Ans.	**Explain working of WWW.** ***(Note: Description explaining the concept shall be considered).*** The Web is a repository of information in which the documents, called **web pages,** are distributed all over the world and related documents are linked together. The WWW today is a distributed client-server service, in which a client using a browser can access a service using a server. The service provided is distributed over many locations called *sites.* Each site holds one or more web pages. Each web page can contain some links to other web pages in the same or other sites. • Simple web page has no links to other web pages. • Composite web page has one or more links to other web pages. Each web page is a file with a name and address. The web page is stored at the web server. Each time a request arrives, the corresponding document is sent to the client.	**4M** ***Explanation 4M***

	(d) Ans.	**Describe the sub-network address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0** To find the subnet address we have to AND the IP address and the subnet mask as shown below: 200.45.34.56 **Destination address:** 11001000 . 00101101 . 00100010.00111000 255.255.240.0 **AND** Subnet mask **11111111 . 11111111 . 1111**0000.00000000 ANDing 200.45.32.0 Subnet address **11001000 . 00101101 . 0010**0000.00000000 Thus subnet address is **200.45.32.0** **OR** To find the subnet address, keep the network bits in the IP address as it is, and make all host bits as 0‟s.:	4M ***Identifying subnet mask/ netid and host id 2M*** ***Correct Answer 2M***

		200.45.34.56 Destination address: 11001000 . 00101101 . 00100010.00111000 With subnet mask as 255.255.240.0, network bits are **20** and host bits are **12.** Keeping first 20 bits as it is, and making host bits as 0, the subnet address is obtained as given below. Subnet address: **11001000 . 00101101 . 0010**0000.00000000 Thus subnet address is **200.45.32.0**	

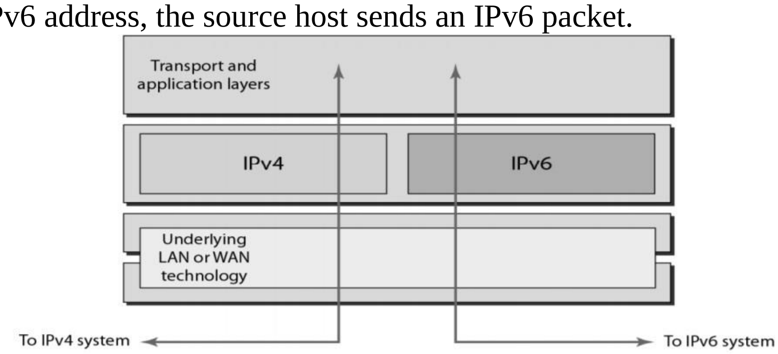
3. **Attempt any THREE of the following:** **12**

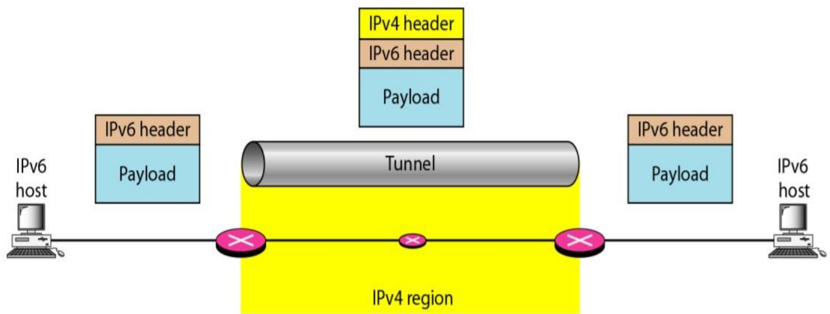
(a) **Explain difference between distance vector and link state routing. (Any four points).** **4M**

Ans.

Sr. No.	Distance Vector Routing	Link State Routing
1	Routing tables are updated by exchanging information with the neighbours.	Complete topology is distributed to every router to update a routing table.
2	It update full routing table.	It updates only link states.
3	It uses Bellman-Ford algorithm	It uses Dijkstra algorithm.
4	Distance Vector routing doesn‟t have any hierarchical structure.	Link state routing works best for hierarchical routing design.
5	CPU and memory utilization is lower than Link state routing.	Higher utilization of CPU and memory than distance vector routing.
6	Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
7	Example protocols are RIP and IGRP.	Example protocols are OSPF and IS-IS.
8	Slow convergence.	Fast convergence.
9	Summarization is automatic	Summarization is manual.
10	Easier to configure	Harder to configure
11	Count to infinity problem	No count to infinity problem

Any four points 1M each

	(b) **Ans.**	**Explain different transition method of IPv4 to IPv6.** Three Transition from IPv4 to IPv6 strategies are 1. Dual Stack 2. Tunnelling 3. Header Translation **1. DUAL STACK** In this kind of strategy a station has a dual stack of protocols run IPv4 and IPv6 simultaneously. To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.  **Fig. Dual Stack** **2. Tunnelling** Tunnelling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. ➢ To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region. ➢ To make it clear that the IPv4 packet is carrying an IPv6 packet as data the protocol value is set to 41.	**4M** ***List 1M*** ***1M for each transition method***



Header Translation

In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header see figure.

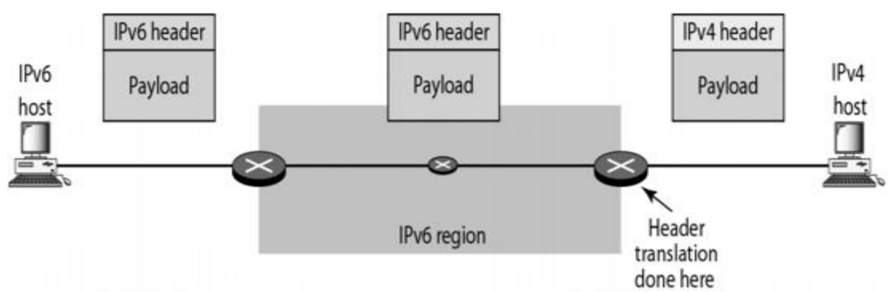
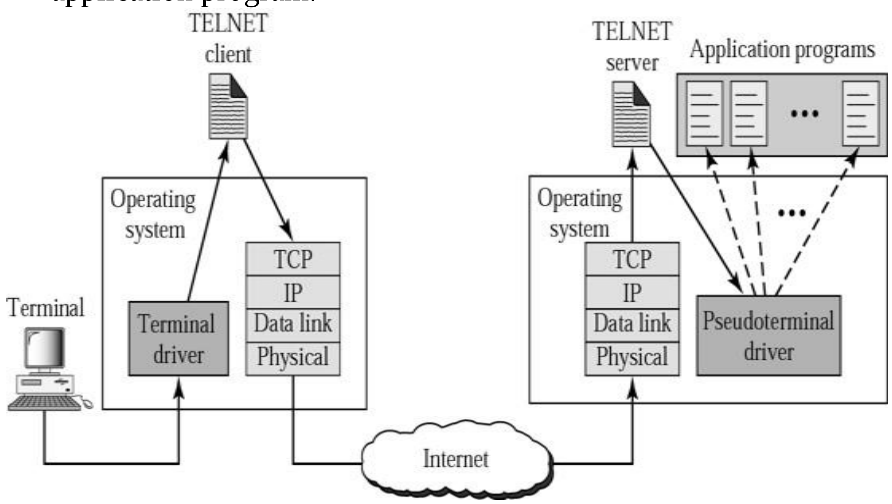


Fig. Header Translation

	(c) **Ans.**	**Explain the working of TELNET.** **TELNET:** TELNET is an abbreviation for TErminaLNETwork. It is the standard TCP/IP protocol for virtual terminal service. **TELNET Working:** • TELNET is a client-server application that allows a user to log on to a remote machine, giving the user access to the remote system. • The user sends the keystrokes to the terminal driver, where the local operating system accepts the characters but does not interpret them. • A terminal driver correctly interprets the keystrokes on the local terminal or terminal emulator. • The characters are sent to the TELNET client, which transforms	**4M** ***Working description 2M***

		the characters to a universal character set called network virtual terminal (NVT) characters and delivers them to the local TCP/IP protocol stack. • The commands or text, in NVT form, travel through the Internet and arrive at the TCP/IP stack at the remote machine. • Here the characters are delivered to the operating system and passed to the TELNET server, which changes the characters to the corresponding characters understandable by the remote computer. • However, the characters cannot be passed directly to the operating system because the remote operating system is not designed to receive characters from a TELNET server: It is designed to receive characters from a terminal driver. • A piece of software called a pseudo terminal driver is added which pretends that the characters are coming from a terminal. • The operating system then passes the characters to the appropriate application program.  **Fig. Working of TELNET**	***Working diagram 2M***

	(d)	**The dump of a UDP header in hexadecimal format is as follows: BC 82000 D 002 B 001 D Obtain the following from it:** **(i) Source port number** **(ii) Destination port number** **(iii) Total length** **(iv) Length of the data**	**4M**

	Ans.	The UDP header has four parts, each of two bytes. That means we get the following interpretation of the header. i) Source port number = **$BC82_{16}$** = **48258** ii) Destination port number = **$000D_{16}$**= **13** iii) Total length = **$002B_{16}$** = **43 bytes** iv) Since the header is 8 bytes the data length is **43 − 8 =35 bytes**.	***Each correct answer carries 1M***

4. **Attempt any THREE of the following:** **12**

(a) **Construct a diagram to show the application of cookies in a scenario in which the server uses cookies for advertisement.** ***(Note: Any other diagram shall be considered)*** **4M**

Ans. **Use of Cookies for advertisements:**

A cookie is also used by advertising agencies. An advertising agency can place banner ads on some main website that is often visited by users. The advertising agency supplies only a URL that gives the banner address instead of the banner itself. When a user visits the main website and clicks on the icon of an advertised corporation, a request is sent to the advertising agency. ***Use 1M***

The advertising agency sends the banner, a GIF file, for example, but it also includes a cookie with the ill of the user.

Any future use of the banners adds to the database that profiles the Web behaviour of the user. The advertising agency has compiled the interests of the user and can sell this information to other parties. This use of cookies has made them very controversial. Hopefully, some new regulations will be devised to preserve the privacy of users.

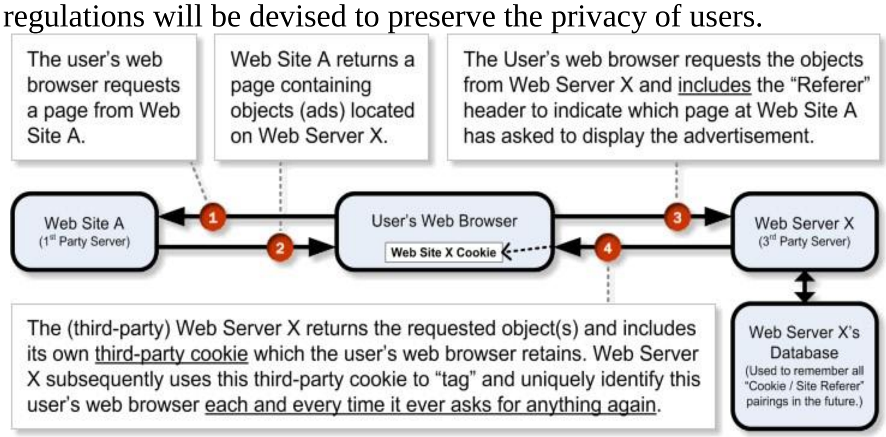
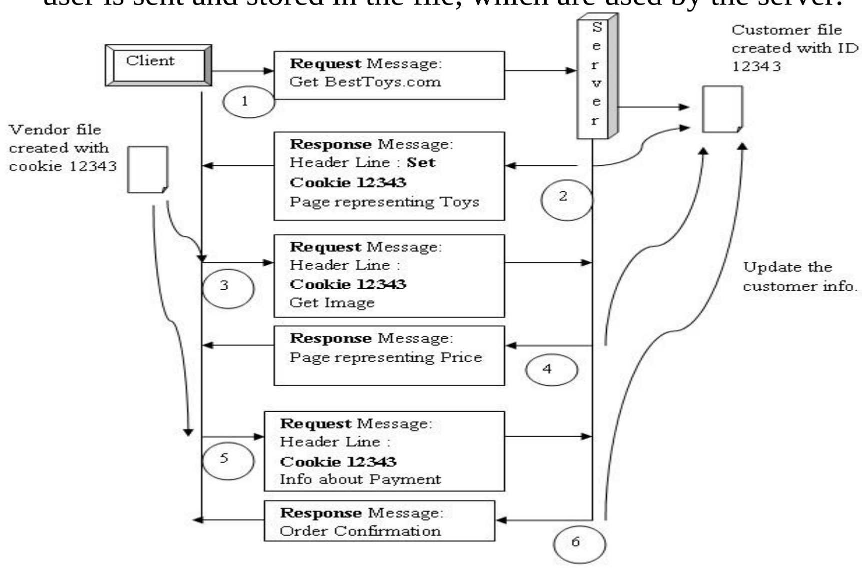


Fig. Use of Cookies in advertisement

OR

		• Figure below shows a scenario in which an electronic store can benefit from the use of cookies. • A shopper wants to buy a toy from an electronic store named BestToys.com. • The Server sends the Webpage, but it also includes a cookie with the ID 12343. • Using this a file is created such that the information clicked by the user is sent and stored in the file, which are used by the server.  	***Diagram 3M***

	(b) **Ans.**	**Describe the RIP message format.** **RIP(Routing Information Protocol) message format** • RIP is routing protocol based on Distance Vector Routing algorithm which is an intradomain (interior) routing protocol used inside an autonomous system. • The metric used by RIP is the distance which is defined as the number of links (networks) that have to be used to reach the destination. For this reason, the metric in RIP is called a hop count. • Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops. • The next node column defines the address of the router to which the packet is to be sent to reach its destination.	**4M** ***Description 2M***

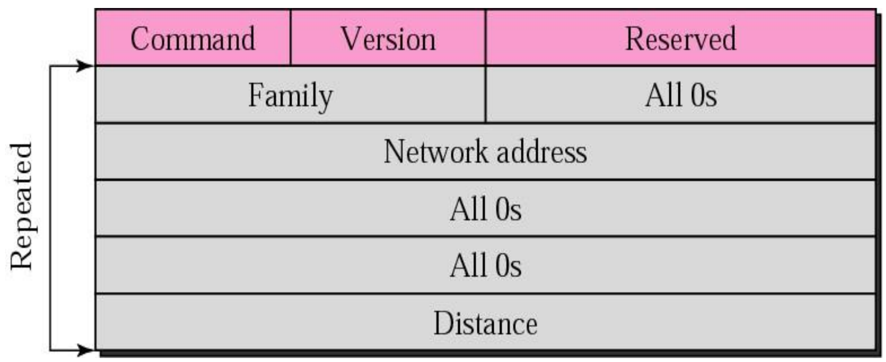


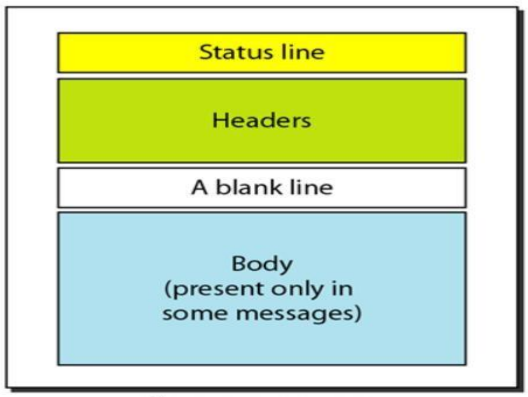
Fig. RIP message format

Message format diagram 2M

- **Command**: 8-bit
  - The type of message: request (1) or response (2)
- **Version:** 8-bit ○ Define the RIP version
- **All 0s** ○ This field is not actually used by RFC 1058 RIP; it was added solely to provide backward compatibility with pre-standard varieties of RIP. Its name comes from its defaulted value, zero.
- **Family:**
  - 16-bit field defines the family of the protocol used. For TCP/IP, value is 2
- **IP Address Network Address:**
  - 14 bytes n Defines the address of the destination network and 14 bytes for this field to be applicable to any protocol. However, IP currently uses only 4 bytes, the rest are all 0s
- **Distance:**
  - 32-bit field defines the hop count from the advertising router to the destination network

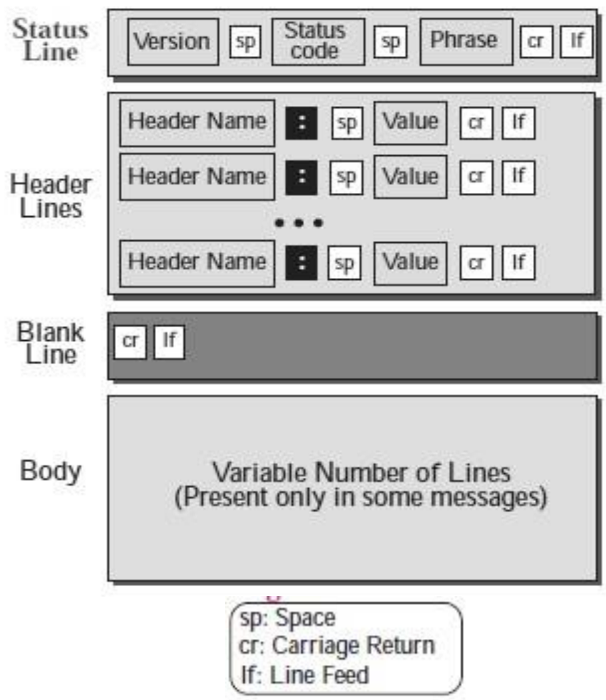
	(c) Ans.	**Describe the HTTP response message format.** ***(Note: Any other diagram showing the actual contents of the format shall be considered).*** **Status Line** Status line shows status for the response it indicates response status using a code as well as a status phrase. The status-Line begins with a protocol version, then status code and status phrase.	**4M** ***Description 2M***

		E.g: HTTP/1.1 200 OK **Headers** Three types of headers are present HTTP Response message which are as follows. **General Header** The general header gives general information about the message and can be present in both a request and a response. e.g. Date: Mon, 27 Jul 2009 12:28:53 GMT **Response Header** The response header can be present only in a response message. It specifies the server's configuration and special information about the request. e.g. Server: Apache/2.2.14 (Win32) **Entity Header** The entity header gives information about the body of the document. e.g. Content-Length: 88 e.g. Content-Type: text/html **Blank Line** An empty line (i.e., a line with nothing preceding the CRLF) indicating the end of the header fields **Body** It contains actual content. This part is optional.	***Diagram 2M***

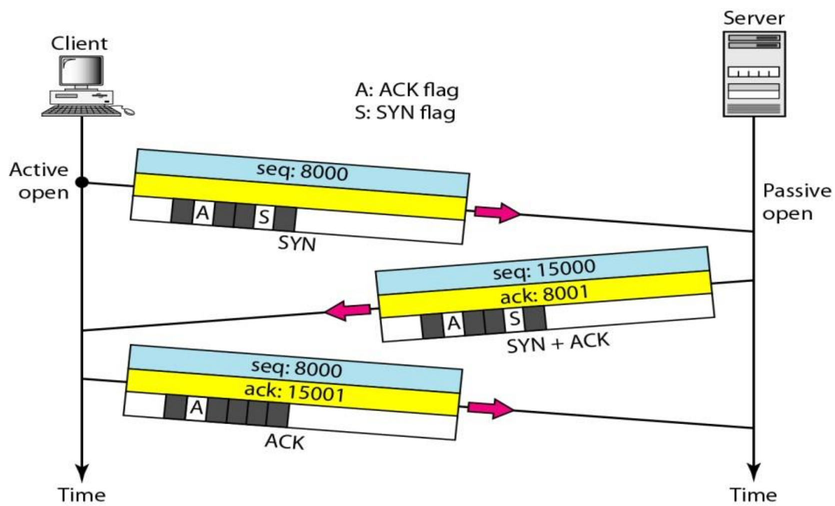


Response message

OR


Status Line
Version
sp
Status code
sp
Phrase
cr
lf
Header Lines
Header Name
:
sp
Value
cr
lf
Blank Line
cr
lf
Body
Variable Number of Lines
(Present only in some messages)
sp: Space
cr: Carriage Return
lf: Line Feed

	(d) **Ans.**	**Explain the TCP connection establishment using a three way handshake mechanism. Connection Establishment** TCP uses a Three way handshaking mechanism to establish a connection between client and server machines. The three steps in three way handshaking mechanism are as follows. **SYN:** The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. **SYN + ACK** The server sends the second segment, a SYN +ACK segment, with 2 flag bits set. **ACK** The client sends the third segment. This is just an ACK segment. It guarantees the completion of three way handshaking.	**4M** ***Each step description carries 1M***

		 **Fig. TCP Connection Establishment : Three way Handshaking**	***Diagram 1M***

	(e) Ans.	**Explain about standard and non standard protocols at the application layer.** ***(Note: Any other protocol shall be considered).*** **HTTP** • The Hypertext Transfer Protocol (HTTP) is a Application layer protocol used mainly to access data on the World Wide Web. • HTTP uses the services of TCP on well-known port 80. **FTP** • FTP (File Transfer Protocol) is standard TCP/IP protocol to transfer files. • It uses the services of TCP. It needs two TCP connections. • The well-known port 21 is used for the control connection and the well-known port 20 for the data connection. **SMTP** • It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP standard protocol. • Using a process called "store and forward," SMTP moves your email on and across networks. • It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. • Port number for SMTP is 25.	**4M** ***Any 4 protocol descripti on 1M each***

		TELNET • TELNET is an abbreviation for TErminaLNETwork. It is the standard TCP/IP protocol for virtual terminal service • TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system. • There are two parties involved TELNET Client and TELNET server. **DNS** • It stands for Domain Name Service. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. • For example, the domain name www.abc.com might translate to 198.105.232.4. • Port number for DNS is 53. **DHCP** • It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts. • There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. • Port number for DHCP is 67, 68. **POP3** • Post Office Protocol, version 3 (POP3) is simple and limited in functionality. • POP works as a Message Access Agent. • The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server. • Mail access starts with the client when the user needs to download e-mail from the mailbox on the mail server.	

5.	 **(a)** **Ans.**	**Attempt any TWO of the following:** **Explain how TCP connections are established using the 3 way handshake. What happens when 2 hosts simultaneously try to establish a connection?** ***(Note: Any other explanation of the concept shall be considered).***	**12** **6M**

Connection Establishment

TCP uses a Three way handshaking mechanism to establish a connection between client and server machines.

The three steps in three way handshaking mechanism are as follows.

SYN:

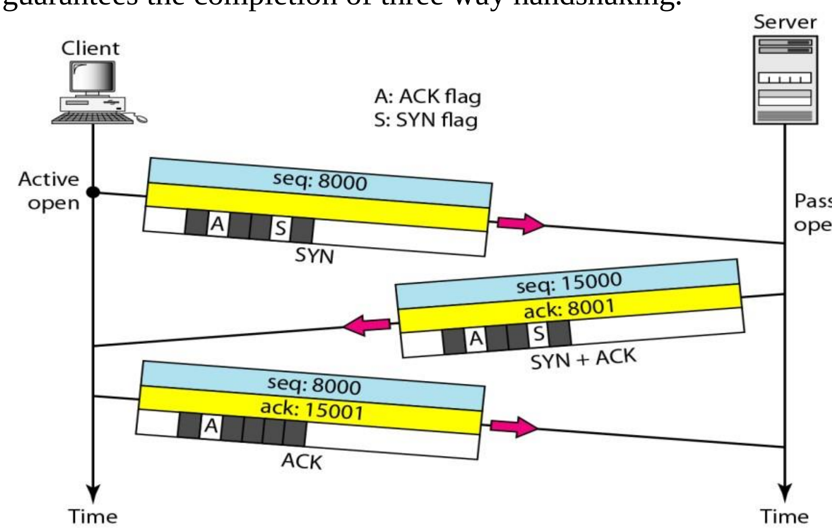
The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers.

SYN + ACK

The server sends the second segment, a SYN +ACK segment, with 2 flag bits set.

ACK

The client sends the third segment. This is just an ACK segment. It guarantees the completion of three way handshaking.



If 2 host Simultaneously try to establish connection:

Simultaneous Open:

- It's possible for two applications to send a SYN to each other to start a TCP connection, although the possibility is small, because both sides have to know which port on the other side to send to.

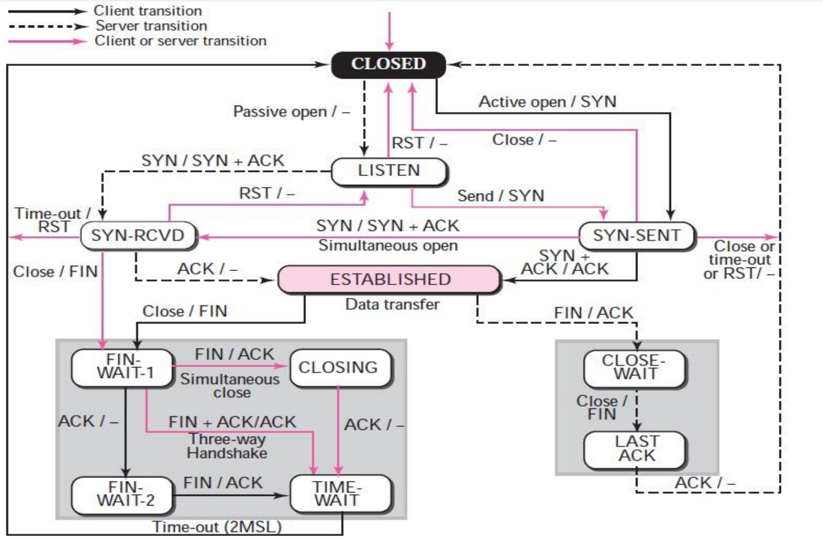
1M Diagram

3M Steps

2M for simultaneous connection

		This process is called "Simultaneous Open", or "simultaneous active open on both sides". • In a simultaneous open, both applications issue active opens. • This is a rare situation in which there is no client or server;	

		communication is between two peers that know their local port numbers. • Both TCPs go through **SYN-SENT** and **SYN-RCVD** states before going to the **ESTABLISHED** state. • Both processes act as client and server. • The two SYN+ACK segments acknowledge the SYN segments and open the connection. **OR** **Simultaneous Close:** • It's permitted in TCP for both sides to do "active close", which is called "Simultaneous Close". During "Simultaneous Close", 4 packets are exchanged, the same as in normal situations. • In this situation, both ends issue an active close. • Both TCPs go to the FIN-WAIT-1 state and send FIN segments that are in transit simultaneously. • After receiving the FIN segment, each end goes to the CLOSING state and sends an ACK segment. • The CLOSING state takes the place of FIN-WAIT-2 or CLOSEWAIT in a common scenario.	

	(b) **Ans.**	**Explain TCP connection management with the help of TCP connection management finite state machine.** ***(Note: Any other explanation of the concept shall be considered).*** 	**6M** ***3M for diagram***

		To keep track of all the different events happening during connection establishment, connection termination, and data transfer, TCP is specified as the **Finite State Machine –FSM** **TCP State Machine:** • TCP uses a three way handshake to close connection • Singled by the FIN bit in the packet header The figure shows the two FSMs used by the TCP client and server combined in one diagram. • Ovals/rectangle represents states. • Transition from one state to another is shown using directed lines. • Each line has two strings separated by a slash. • The first string is the input, what TCP receives. • The second is the output, what TCP sends. • The dotted black lines in the figure represent the transition that a server normally goes through; • The solid black lines show the transitions that a client normally goes through. • Sometimes in some situations, a server transitions through a solid line or a client transitions through a dotted line.	***3M for explanation of steps***

State	Description
CLOSED	No connection exists
LI STEN	Passive open received; waiting for SYN
SYN- SENT	SYN sent; waiting for ACK
SYN- RCVD	SYN+ACK sent; waiting for ACK
ESTABLI SHED	Connection established; data transfer in progress
FI N- WAI T- 1	First FIN sent; waiting for ACK
FI N- WAI T- 2	ACK to first FIN received; waiting for second FIN
CLOSE- WAI T	First FIN received, ACK sent; waiting for application to close
TI ME- WAI T	Second FIN received, ACK sent; waiting for 2MSL time-out
LAST- ACK	Second FIN sent; waiting for ACK
CLOSI NG	Both sides decided to close simultaneously

(c) **Explain the addressing scheme in IPv4 and IPv6. When IPv6 protocol is introduced, does the ARP protocol have to be changed? Explain in details.** **6M**

Ans.

<u>An IPv4 Address:</u>

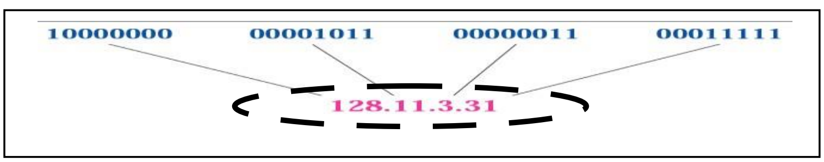
- ✓ An IP address is a 32-bit address.
- ✓ The IP addresses are unique.

IPv4 2M

Address space rule

- ✓ The address space in a protocol That uses N-bits to define an Address is = 2^N
- ✓ ***The address space of IPv4 is 2^{32}or4,294,967,296.*** **Address Space Notations**:
- **Binary Notation :**

  01110101 10010101 00011101 11101010
- **Dotted-decimal notation**



Dotted-decimal notation

- **Hexadecimal Notation**

0111 0101	1001 0101	0001 1101	1110 1010
75	**95**	**1D**	**EA**

Hexadecimal Notation

10000001	00001011	00001011	11101111
129.11.11.239			

IPv6 2M

Example of Dotted-decimal Notation.

<u>IPv6 Address Representation Examples</u>:

2031:0000:130F:0000:0000:09C0:876A:130B
2031:0:130f::9c0:876a:130b

ARP 2M

		FF01:0:0:0:0:0:0:1 >>> FF01::1 0:0:0:0:0:0:0:1 >>> ::1 0:0:0:0:0:0:0:0 >>> ::	

		Notations in 128 bit • Dotted decimal 123.145.20.34 • hexadecimal notation. 23BA:1234:00B1:0000:BF30:3456:000A:FFFF • Mixed representation 23BA:1234:123:56:BF30:3456:000A:FFFF • CIDR notation. FDC1:AB23:0:FFFF/27 • $3.4 * 10^{38}$ possible addressable nodes • $5 * 10^{28}$ addresses per person	

<table>
<tr><td>6.</td><td>
(a)

Ans.</td><td>Attempt any TWO of the following:
Explain the 3 intra domain routing protocols.
(Note: Explanation of any other protocols shall be considered). i)
Distance Vector Routing:
- Require only local state (less overhead smaller footprint)
- Harder to debug
- Can suffer from loops
• Distance vector Routing Protocol:
• Here Distance vector:
✓ Current best known cost to reach a destination
✓ Idea: exchange vectors among neighbors to learn about lowest cost paths.
✓ Distance vector protocols advertise their routing table to all directly connected neighbors at regular frequent intervals using a lot of bandwidth and are slow to converge.
✓ When a route becomes unavailable, all router tables must be updated with that new information.
✓ The problem is with each router having to advertise that new information to its neighbors, it takes a long time for all routers to have a current accurate view of the network.
✓ Distance vector protocols use fixed length subnet masks which aren"t scalable.
- periodically (on the order of several seconds to minutes)
- whenever table changes (called triggered update)
• Each update is a list of pairs:
- (Destination , Cost)
• Update local table if receive a "better" route - smaller cost
- from newly connected/available neighbor</td><td>12
6M

Any 3 protocols 2M each</td></tr>
</table>

• Refresh existing routes; delete if they time out
i.e. RIP-Routing Information Protocol

ii) Link State Routing:

- Have a global view of the network
- Simpler to debug
- Require global state

Link State Strategy

- each router shares the information/knowledge of its neighborhood with every other router in the internetwork.
- Send to all nodes (not just neighbors)
- Send only information about directly connected links not entire routing table)

Link State Packet (LSP)

- ID of the node that created the LSP
- Cost of link to each directly connected neighbor
- Sequence number (SEQNO)

Time-to-live (TTL) for this packet

i.e. OSPF-Open Shortest Path First

iii) RIPv2:

_ Runs over UDP port 520
_ Limits networks to 15 hops (16 = 1)
_ Depends on count to infinity for loops
_ Supports split horizon, poison reverse
_ RFC 1812 specifies what options routers should or must have.

iv) MOSPF *(*Multicast Open Shortest Path First):

- This protocol is an extension of the OSPF protocol that uses multicast link state routing to create source-based trees.
- The protocol requires a new link state update packet to associate the unicast address of a host with the group address or addresses the host is sponsoring. This packet is called the group membership LSA. In this way, we can include in the tree only

		the hosts (using their unicast addresses) that belong to a particular group. • Thus a tree that contains all the hosts belonging to a group, but we use the unicast address of the host in the calculation. • For efficiency, the router calculates the shortest path trees on	

demand (when it receives the first multicast packet).

- In addition, the tree can be saved in cache memory for future use by the same source/group pair.
- MOSPF is a **data-driven** protocol; the first time an MOSPF router sees a datagram with a given source and group address, the router constructs the Dijkstra shortest path tree.

v) Multicast Distance Vector Routing (DVMRP):

The **Distance Vector Multicast Routing Protocol (DVMRP)** is an implementation of multicast distance vector routing. It is a source-based routing protocol, based on RIP.

- Unicast distance vector routing is very simple; extending it to support multicast routing is complicated.
- Multicast routing does not allow a router to send its routing table to its neighbors.
- The idea is to create a table from scratch using the information from the unicast distance vector tables.
- Multicast distance vector routing uses source-based trees, but the router never actually makes a routing table.
- When a router receives a multicast packet, it forwards the packet as though it is consulting a routing table.
- After its use (after a packet is forwarded) the table is destroyed.
- To accomplish this, the multicast distance vector algorithm uses a process based on four decision-making strategies.

vi) PIM-DM (Protocol Independent Multicast, Dense Mode):

- PIM-DM is used when there is a possibility that each router is involved in multicasting (dense mode).
- In this environment, the use of a protocol that broadcasts the packet is justified because almost all routers are involved in the process.
- PIM-DM is a source-based tree routing protocol that uses RPF and pruning/grafting strategies for multicasting.
- Its operation is like DVMRP; however, unlike DVMRP, it does not depend on a specific unicasting protocol.

		• It assumes that the autonomous system is using a unicast protocol and each router has a table that can find the outgoing	

		interface that has an optimal path to a destination. This unicast protocol can be a distance vector protocol (RIP) or link state protocol (OSPF).	

	(b) **Ans.**	**Describe modern computer use dynamic routing. Explain with example how distance vector routing is used to route the packet & why count-to-infinity problem arises and how does it get solved?** ***(Note: Any other description of the concept shall be considered.)*** **Dynamic routing** uses a dynamic routing protocol to automatically select the best route to put into the routing table. So instead of manually entering static routes in the routing table, dynamic routing automatically receives routing updates, and dynamically decides which routes are best to go into the routing table. This intelligent and hands-off approach that makes dynamic routing so useful in modern era. Dynamic routing protocols vary in many ways and this is reflected in the various administrative distances assigned to routes learned from dynamic routing. These variations take into account differences in reliability, speed of convergence, and other similar factors. **Distance vector routing:** 1. Distance Vector Routing is one of the dynamic routing algorithm. 2. It is suitable for packet switched network. 3. In distance vector routing, each router maintains a routing table. 4. It contains one entry for each router in the subnet. 5. This entry has two parts: a. The first part shows the preferred outgoing line to be used to reach the destination. b. Second part gives an estimate of the time or distance to the destination. In distance vector routing, a node tells its neighbor about its distance to every other node in the network. **Count to infinity problem:** 1. One of the important **issue** in Distance Vector **Routing** is Count to **Infinity Problem**. 2. **Count to infinity** is just another name for a **routing** loop. 3. In distance vector **routing**, **routing** loops usually occur when an	**6M** ***2M for Dynamic routing concept*** ***2M for Distance vector routing and*** ***1M for Count to infinity***

			proble m

interface goes down.
4. It can also occur when two **routers** send updates to each other at the same time.

OR

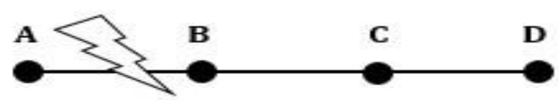
For a routing protocol to work properly, if a link is broken (cost becomes infinity), every other router should be aware of it immediately, but in distance vector routing, this takes some time. The problem is referred to as **count to infinity.** It takes several updates before the cost for a broken link is recorded as infinity by all routers.

1M for solution

Count to infinity problem can be solved by following methods:
1. Defining Infinity
2. Split Horizon
3. Split Horizon an Poison Reverse

Example:

Link Between A & B is Broken



	A	B	C	D
A	0, -	1, A	2, B	3, C
B	1, B	0, -	2, C	3, D
C	2, B	1, C	0, -	1, C
D	3, B	2, C	1, D	0, -

Imagine a network with a graph as shown above in figure 4.8.
- As you see in this graph, there is only one link between A and the other parts of the network.
- Now imagine that the link between A and B is cut.
- At this time, B corrects its table.
- After a specific amount of time, routers exchange their tables, and so B receives C's routing table.

		• Since C doesn't know what has happened to the link between A and B, it says that it has a link to A with the weight of 2 (1 for C to B, and 1 for B to A -- it doesn't know B has no link to A). • B receives this table and thinks there is a separate link between	

C and A, so it corrects its table and changes infinity to 3 (1 for B to C, and 2 for C to A, as C said).

- Once again, routers exchange their tables.
- When C receives B's routing table, it sees that B has changed the weight of its link to A from 1 to 3, so C updates its table and changes the weight of the link to A to 4 (1 for C to B, and 3 for B to A, as B said).
- This process loops until all nodes find out that the weight of link to A is infinity.
- This situation is shown in the table below
- In this way, Distance Vector Algorithms have a slow convergence rate.
- One way to solve this problem is for routers to send information only to the neighbors that are not exclusive links to the destination.

	B	C	D
Sum of Weight to A after link cut	∞, A	2, B	3, C
Sum of Weight to A after 1st updating	3, C	2, B	3, C
Sum of Weight to A after 2nd updating	3, C	4, B	3, C
Sum of Weight to A after 3rd updating	5, C	4, B	5, C
Sum of Weight to A after 4th updating	5, C	6, B	5, C
Sum of Weight to A after 5th updating	7, C	6, B	7, C
Sum of Weight to A after nth updating	…..	….	….
∞	∞	∞	∞

	(c) **Ans.**	**Describe E-mail security over non-secure channel.** ***(Note: Any other explanation on email security shall be considered.)*** Email security describes different techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss or compromise.	**6M**

		Email is often used to spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to part with sensitive information, open attachments or click on hyperlinks that install malware on the victim‟s device.	

		• Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than intended recipients. Email encryption often includes authentication. Email allows attackers • to use it as a way to cause problems in attempt to profit. Whether through spam campaigns, malware and phishing attacks, sophisticated targeted attacks, or business email compromise (BEC), attackers try to take advantage of the lack of security of email to carry out their actions. • Since most organizations rely on email to do business, attackers exploit email in an attempt to steal sensitive information. • Because email is an open format, it can be viewed by anyone who can intercept it. It can be easily read and the contents of an email by intercepting it. • Email Security Policies can be established by viewing the contents of emails flowing through their email servers. It‟s important to understand what is in the entire email in order to act appropriately. After these baseline policies are put into effect, an organization can enact various security policies on those emails. • These email security policies can be as simple as removing all executable content from emails to more in-depth actions, like sending suspicious content to a sandboxing tool for detailed analysis. • If security incidents are detected by these policies, the organization needs to have actionable intelligence about the scope of the attack. • Enforce email encryption policies to prevent sensitive email information from falling into the wrong hands. • An email gateway scans and processes all incoming and outgoing email and makes sure that threats are not allowed in. • Because attacks are increasingly sophisticated, standard security measures, such as blocking known bad file attachments, are no longer effective.	***Any 6 points 1M each***

		Deploy a secure email gateway that uses a multi-layered approach. It‟s also important to deploy an automated email encryption solution as a best practice. This solution should be able to analyze all outbound email traffic to determine whether the material is sensitive. If the content is sensitive, it needs to be encrypted before it is emailed to the intended recipient. This will prevent attackers from viewing emails, even if they were to intercept them. The Pretty Good Privacy (PGP) provides e-mail with privacy, integrity, and authentication can be used over non secure channel such as internet. It is used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions and to increase the security of e-mail communications. Another security service designed for electronic mail is Secure/Multipurpose Internet Mail Extension (S/MIME). The protocol is an enhancement of the Multipurpose Internet Mail Extension (MIME) protocol. This allows user to digitally sign the email to enhance privacy and data security.	

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

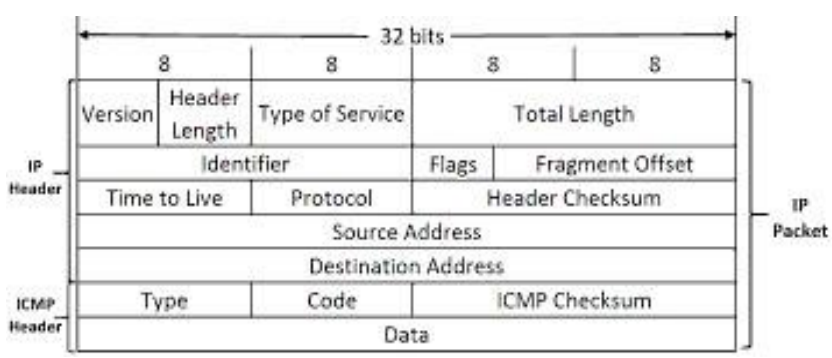
SUMMER – 2023 EXAMINATION

MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code: 22520**

Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills.
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for anyequivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

Q. No	Sub Q.N.	Answer	Marking Scheme
1.		**Attempt any FIVE of the following:**	**10**
	a)	**Draw and label sketch of ICMPV4 packet format.**	**2M**
	Ans.	**ICMPV4 packet format** 	*Correct labelled diagram 2M*

8) As per the policy decision of Maharashtra State Government, teaching in English/Marathi and Bilingual (English + Marathi) medium is introduced at first year of AICTE diploma Programme from academic year 2021-2022. Hence if the students in first year (first and second semesters) write answers in Marathi or bilingual language (English +Marathi), the Examiner shall consider the same and assess the answer based on matching of concepts with model answer.

Subject: Advanced Computer Network (Elect) **Subject Code: 22520**

	b) **Ans.**	**State the importance of IPV6 and IPC4.** **Importance of IPV6 over IPV4 (any two) i) huge number of IP addresses:** IPv6 has 128-bit addresses when compared to 32-bit addresses of IPv4 which results in a very large increase in the availability of IP addresses and creates a lot of advantages. **ii) End to End Connectivity:** IPv6 eliminates the need for NAT which results in better connectivity in peer-peer networks. **iii) Interoperability:** IPv6 promotes interoperability between different IPv6 implementations. **iv) Built-in Security:** IPv6 provides authentication and encryption.	**2M** *Any two points 1M each for relevant contents*

	c) **Ans.**	**Distinguish between SMTP and POP3 protocol (Any two points)**	**2M** *Any two points 1M each for relevant contents*

Parameter	SMTP	POP3
Full form	Simple Mail Transfer Protocol (SMTP).	Post Office Protocol 3 (POP 3)
Designed	SMTP is designed for sending the mails.	POP3 has been designed for receiving the mails.
Implementation	SMTP is implemented technically and physically on port number 25 of the system.	POP3 is implemented on port number 110.
Known as	SMTP is also known as the PUSH protocol.	POP3 is also known as POP protocol
Type	SMTP acts as a MTA (Message Transfer Agent) for sending the message to the receiver.	POP3 is a MAA (Message Access Agent) for accessing the messages from mailboxes.

Target Usage	SMTP transfers the mail from the sender's computer to the mailbox present on the receiver's mail server.	POP3 allows you to retrieve and organize mail from the mailbox on the receiver mail server to the receiver's computer.

d) What is UDP? Which services are provided by UDP (Any two)? — **2M**

Ans.

UDP(User Datagram Protocol):

UDP is a simple, datagram-oriented, transport layer protocol. It involves a minimum amount of communication mechanisms. It is a connectionless, reliable protocol.

UDP Services:

1. Process-to-Process Communication: - UDP provides process-toprocess communication using socket addresses, a combination of IP addresses and port numbers.
2. Connectionless Service: - UDP provides a connectionless service, i.e. each user datagram sent by UDP is an independent datagram.
3. UDP provides no flow control.
4. UDP does not provides no error control.
5. UDP does not provide congestion control.
6. UDP protocol encapsulates and decapsulates messages.

Definition 1M

Any two services 1M

e) State importance of Routing table. — **2M**

Ans.

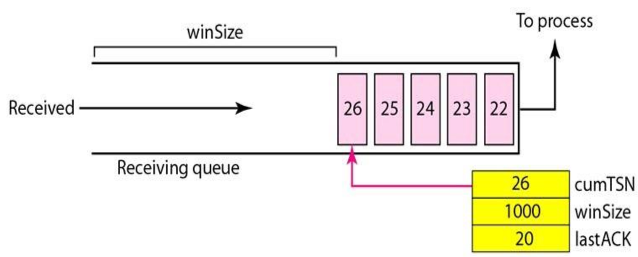
Importance of Routing table

- Routing tables are essential in the routing because they maintain a map of connected networks, which ensures that the process of forwarding packets is as efficient as possible.
- Without the presence of routing tables, routers would have no idea how to get packets to their intended destinations.

Correct explanation 2M

	f) **Ans.**	**State the use of Telnet.** Followings are some of the uses of Telnet • TELNET is used to connect remote computers and issue commands on those computers. • It is used as a standard TCP/IP protocol for virtual terminal service which is given by ISO. • Telnet can be used to test or troubleshoot remote web or mail servers, as well as trusted internal networks.	**2M** ***Any two uses 1M each***

	g) **Ans.**	**State the concept of fragmentation in IPV4.** **The concept of fragmentation in IPV4** Fragmentation: When the maximum size of datagram is greater than maximum size of data that can be held a frame then the network layer divides the datagram received from x-port layer into fragments. **OR** Fragmentation is the division of an IP datagram into smaller units. After fragmentation, each fragment will have its own header with few fields changed and few fields remaining the same. **OR** In fragmentation, a datagram is divided into smaller units. Most of the fields of the original header are copied into the fragment header. The three fields' Flags, Fragmentation offset and Total length are altered	**2M** ***Correct concept 2M*** ***Example given as fragmentation may be considered***

2.		**Attempt any <u>THREE</u> of the following:**	**12**
	a)	**Describe flow control under SCTP.**	**4M**
	Ans.	***(Any other relevant explanation or example can be considered)*** **Flow control under SCTP** Flow control in SCTP is similar to that in TCP. Like TCP, SCTP executes flow control to prevent overwhelming the receiver. In SCTP, we need to handle two units of data, the byte and the chunk. The values of rwnd and cwnd are expressed in bytes; the values of TSN and acknowledgments are expressed in chunks. Current SCTP implementations still use a byte-oriented window for flow control. **Receiver Site:** The receiver has one buffer (queue) and three variables. The queue holds the received data chunks that have not yet been read by the process. The first variable holds the last TSN received,cumTSN. The second variable holds the available buffer size; winsize. The third variable holds the last accumulative acknowledgment, lastACK. The following figure shows the queue and variables at the receiver site.  	***Relevant Explanation of receiver 2M*** ***Relevant Explanation of sender 2M***

SUMMER – 2023 EXAMINATION

MODEL ANSWER

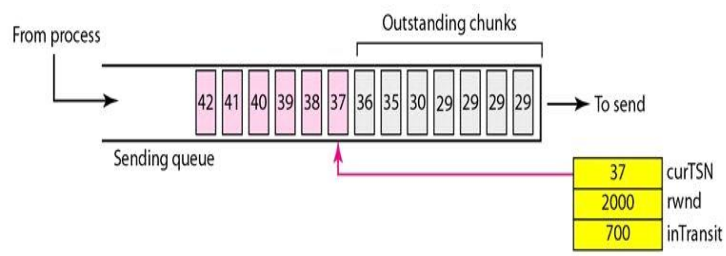
Subject: Advanced Computer Network (Elect) **Subject Code: 22520**

1. When the site receives a data chunk, it stores it at the end of the buffer (queue) and subtracts the size of the chunk from winSize. The TSN number of the chunk is stored in the cumTSN variable.
2. When the process reads a chunk, it removes it from the queue and adds the size of the removed chunk to winSize (recycling).
3. When the receiver decides to send a SACK, it checks the value of lastAck; if it is less than cumTSN, it sends a SACK with a cumulative TSN number equal to the cumTSN. It also includes the value of winSize as the advertised window size.

Sender Site:

The sender has one buffer (queue) and three variables: curTSN, rwnd, and inTransit, as shown in the following figure. We assume each chunk is 100 bytes long.

The buffer holds the chunks produced by the process that either have been sent or are ready to be sent. The first variable, curTSN, refers to the next chunk to be sent. All chunks in the queue with a TSN less than this value have been sent, but not acknowledged; they are outstanding. The second variable, rwnd, holds the last value advertised by the receiver (in bytes). The third variable, inTransit, holds the number of bytes in transit, bytes sent but not yet acknowledged. The following is the procedure used by the sender.



1. A chunk pointed to by curTSN can be sent if the size of the data is less than or equal to the quantity rwnd - inTransit. After sending the chunk, the value of curTSN is incremented by 1 and now points to the next chunk to be sent. The value of inTransit is incremented by the size of the data in the transmitted chunk.

		2. When a SACK is received, the chunks with a TSN less than or equal to the cumulative TSN in the SACK are removed from the queue and discarded. The sender does not have to worry about them anymore.	

		The value of inTransit is reduced by the total size of the discarded chunks. The value of rwnd is updated with the value of the advertised window in the SACK.	
	b) **Ans.**	**What is Mobile IP? List and explain components of Mobile IP.** **Mobile IP:** Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without the user's sessions or connections being dropped. Mobile IP is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. **Components of Mobile IP** **1. Mobile Node(MN): -** Mobile Node (MN) is the hand-held communication device that the user carries. There are devices such as cell phones, PDA or laptops whose software enables network roaming capabilities. **2. Home Agent (HA): -** It is a router on the home network serving as the anchor point for communication with mobile nodes. It tunnels packet from a device on internet, called a correspondent node to a roaming mobile node. **3. Foreign Agent (FA): -** It is a router that may function as the point of attachment for MN when it roams to a foreign network delivering packets from the Home agent to mobile nodes. **4. Correspondent Node (CN): -** Correspondent Node (CN) is a device on the internet communicating to the mobile node. End host to which MN is corresponding (e.g. web server).	**4M** ***Definition 1M*** ***Listing 1M*** ***Explanation 2M for relevant contents***

	c) Ans.	**Describe DHCP with its operation and static and dynamic allocation** ***(Any relevant explanation can be considered)*** DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP. **Working of DHCP:** In a network, a DHCP server manages a pool of IP addresses, as well as default gateway details, DNS details and other information for the clients' network configuration. When a new computer is introduced	**4M** ***DHCP Operation 2M*** ***Static allocation 1M***

		into a DHCP server-enabled network, it will send a query to the DHCP server requesting all the necessary information. When the query reaches the DHCP server, it will grant the new computer a new IP address and a lease - a time frame for which the computer can use this IP address, as well as other configuration details. The whole process takes place immediately after the new computer boots, and to be successful, it has to be completed before initiating IP based communication with other hosts in the network. **Dynamic allocation** When the DHCP server is configured to use dynamic allocation, this means that it uses a lease policy. This way, when an assigned IP address from the available pool is no longer used, it will be transferred back to the pool, making it available for someone else to use. The advantage of this method is that the IP addresses are used to their maximum - as soon as they are no longer used by the client, they are instantly made available to others. The disadvantage of this method is that a client will always have a random IP address. **Static allocation** The static allocation method is very popular in modern ISP networks, which do not use dial-up methods. With the static allocation, the DHCP sever keeps a database with all clients' LAN MAC addresses and gives them an IP address only if their MAC address is in the database. This way, the clients can be sure that they will be getting the same IP address every time. A DHCP server can be set to work using a combination of the allocation methods. For example, in a public Wi-Fi network, all of the known hosts and permanent clients can use the static allocation, whereas for guests, the dynamic allocation is used. This way, known hosts can always use the same IP address and the IP address pool is equally available to everyone.	***Dynamic allocation 1M***

	d) Ans.	**Give use of OSPF with its reason.** **Following are the uses of OSPF with its reason** Link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements.	**4M** ***Any four uses with reasons 1M each***

		• To handle routing efficiently and on time, this protocol divides an autonomous system into areas. • As the name suggested "shortest path first", OSPF calculates the shortest route to a destination through the network based on an algorithm. It uses the Dijkstra algorithm for calculating the shortest path. • Authentication type: There are two types of authentications, i.e., 0 and 1. Here, 0 means for none that specifies no authentication is available and 1 means for password that specifies the passwordbased authentication. • Area identification: It defines the area within which the routing takes place.	

<table>
<tr><td>3.</td><td>
a)

Ans.</td><td>Attempt any <u>THREE</u> of the following:
State significance of following related to IPV6
• Auto configuration
• Renumbering
1. Auto Configuration:
Nodes can connect to a network and automatically generate global IPv6 addresses without the need for manual configuration or help of a server, such as a Dynamic Host Configuration Protocol (DHCP) server.

-When a host in IPv6 joins a network, it can configure itself using the following process:
• Generate a link local address:
The device generates a link local address, which has 10 bits link local prefix (1111 1110 10), followed by 54 zeros, and followed by the 64bit interface identifier, which any host knows how to generate it from its interface card. The result is a 128-bit link local address.

• Test the uniqueness of a link local address:
The node tests to make sure that the link local address that it generates is not already in use on the local network. The node sends a neighbour solicitation message by using the ND (Neighbour Discovery) protocol. In response, the local network listens for a neighbour advertisement message, which indicates that another device is already using the linklocal address. If so, either a new link local address must be generated or auto-configuration fails, and another method must be used.</td><td>12
4M

Explanation of Auto configuration 2M

Explanation of Renumbering 2M

Any relevant explanation can be considered</td></tr>
</table>

- **Assign a link local address:**

If the device passes the uniqueness test, the device assigns the link- local address to its IP interface. The link-local address can be used for communication on the local network but not over the Internet.

- **Contact the router:**

The node tries to contact a local router for more information about continuing the configuration. This contact is performed either by listening for router advertisement messages sent periodically by the routers or by sending a specific router solicitation message to ask a router for information about what to do next.

- **Provide direction to the node:**

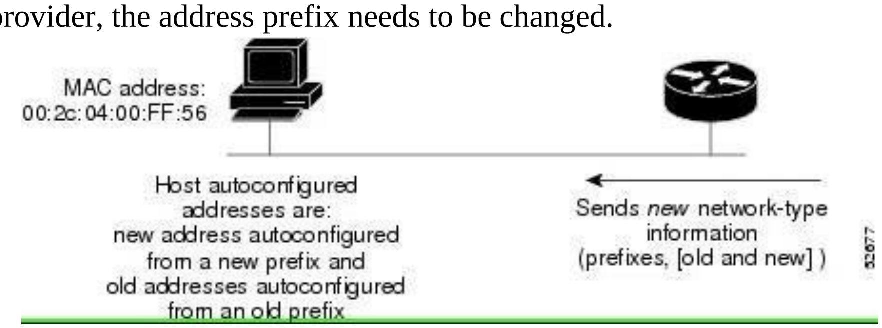
The router provides direction to the node about how to proceed with auto-configuration. Alternatively, the router tells the host how to determine the global Internet address.

- **Configure the global address:**

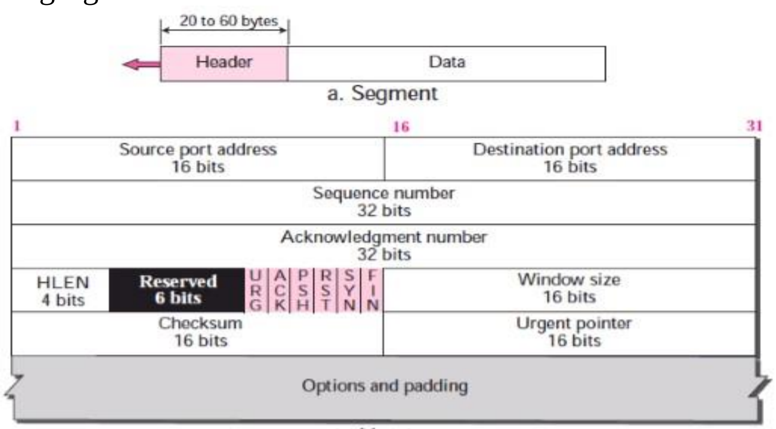
The host configures itself with its globally unique Internet address. This address is generally formed from a network prefix provided to the host by the router.

2. Renumbering:

To allow sites to change the service provider, renumbering of the address prefix (n) was built into IPv6 addressing. Each site is given a prefix by the service provider to which it is connected. If the site changes the provider, the address prefix needs to be changed.



		A router to which the site is connected can advertise a new prefix and let the site use the old prefix for a short time before disabling it. In other words, during the transition period, a site has two prefixes. The main problem in using the renumbering mechanism is the support of the DNS, which needs to propagate the new addressing associated with a domain name.	

	b) Ans.	**Draw and explain TCP segment structure.** TCP is a reliable connection- oriented protocol i.e., connection is established between the sender and receiver before the data can be transmitted. A Packet in TCP is called a segment. TCP segment consists of data bytes to be sent and a header that is added to the data by TCP as shown in following figure.  The header of TCP segment can range from 20-60 bytes.40 bytes are for option. if there are no options, header is of 20 bytes else it can be of upmost 60 bytes. **Header Fields in TCP Segment Structure:** **1) Source port address: -** This is a 16-bit field that defines the port number of the application program in the host that is sending the segment. This serves the same purpose as the source port address in the UDP header.	**4M** *Diagram 1M* *Explanation 3M* *Any other relevant explanation shall be considered*

2) Destination port address: -
This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment. This serves the same purpose as the destination port address in the UDP header.

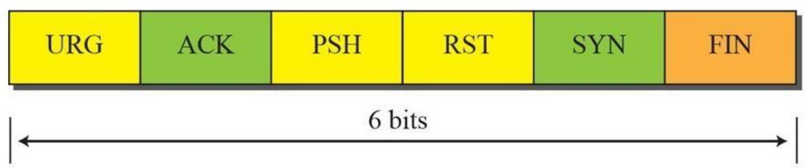
3) Sequence Number: -
This 32-bit field defines the number assigned to the first byte of data contained in this segment. As we said before, TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence comprises the first byte in the segment. During connection establishment, each party uses a random number generator to create an initial sequence number (ISN), which is usually different in each direction.

4) Acknowledgment Number: -
This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number x from the other party, it defines x + 1 as the acknowledgment number. Acknowledgment and data can be piggybacked together.

5) Header length: -
This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 (5 x 4 = 20) and 15 (15 x 4 = 60).

6) Reserved:-
This is a 6-bit field reserved for future use.

7) Control Field:-
This field defines 6 different control bits or flags. These are 6, 1 bit control bits that controls connection establishment, connection termination, connection abortion, flow control, mode of transfer etc.



The function of control fields in TCP are:
URG: Urgent pointer is valid.
PSH: Request for push.
RST: Reset the connection.
SYN: Synchronize sequence numbers.
FIN: Terminate the connection.

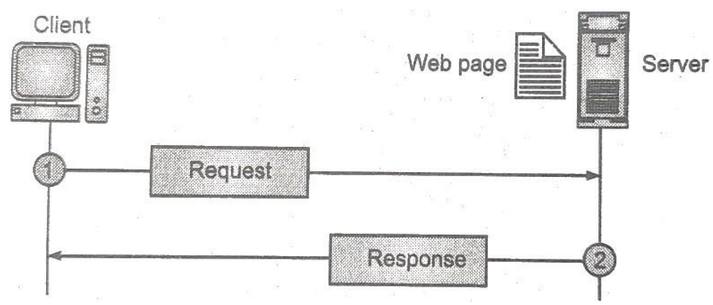
8) **Window Size:** This field tells the window size of the sending TCP in bytes.

9) **Checksum:** This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.

10) **Urgent Pointer:** This field (valid only if the URG control flag is set) used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.

11) **Options:** There can be up to 40 bytes of optional information in the TCP header.

	c) **Ans.**	**With the help of Diagram, explain architecture of WWW.** The WWW (World Wide Web) is a way of exchanging information between computers on the Internet. WWW works on client server architecture, in which a client using a browser can access a service using a server. Today, the WWW is a distributed client server service. The service provided is distributed over many locations called sites and each site holds one or more documents i.e., Web pages.	**4M** ***Diagram 2M*** ***Explanation 2M***



Client sends a request through its browser to the server using HTTP protocol which specifies the way the browser and web server communicates.

Then server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.

Now the browser receives the web page, it interprets it and display the contents of web page in web browser's window.

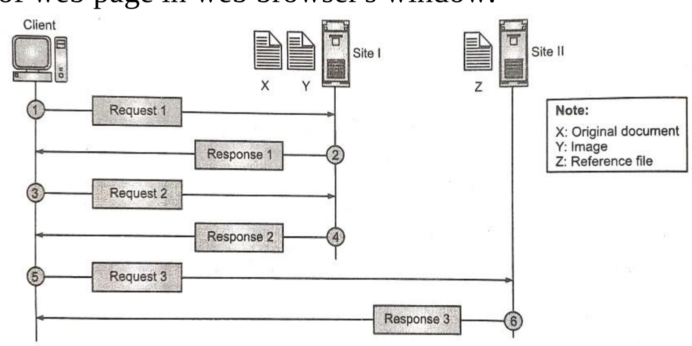


Fig. shows how WWW works.

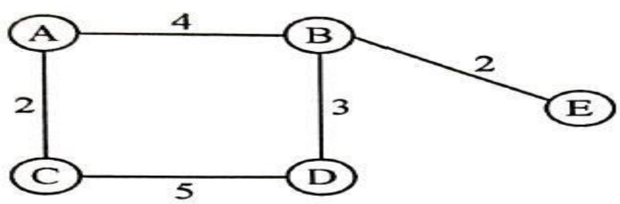
The main web document and the image are stored in two separate files in the same site (file X and file Y) and the referenced text file is stored in another site (file Z).

Since, we are dealing with three different files, (namely, X, Y and Z) we need three transactions if we want to see the whole document. The first

		transaction (request/response) retrieves a copy of the main document (file X), which has a reference (pointer) to the second and the third files. When a copy of the main document is retrieved and browsed, the user	

		can click on the reference to The image to invoke the second transaction and retrieve a copy of the image (file Y). if the user further needs to see the contents of the referenced text file, she can click on its reference pointer) invoking the third transaction and retrieving a copy of the file Z. Note that although file x and y both are stored in site x, they are independent files with different names and addresses. Two transactions are needed to retrieve them.	

	d)	**Use Bellman-ford algorithm to find the shortest distance for all node in the graph.**	**4M**



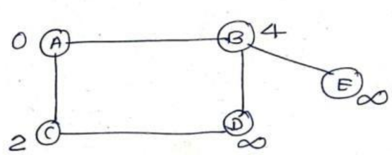
Ans.

For each correct step 1M

Step1:- Let the given source vertex be "0"
Initialise all the distance as infinite,
except the distance to the source itself.
Total no. of vertices in the graph is 5,
so all edges must be proceded 4 times.

A	B	C	D	E
0	∞	∞	∞	∞

Step2:- Let all the edges, are proced with the following order.
(B,E), (B,D), (A,B), (A,C), (C,D)



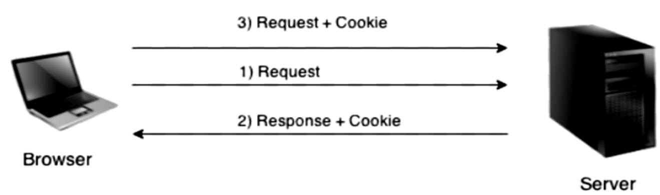
A	B	C	D	E
0	∞	∞	∞	∞
0	∞	2	∞	∞
0	4	2	∞	∞

Step 3 :- The first iteration gurantees to give all the shortest path which are almost 1 edge long, we get the following distance when all edges are proceed second time.

A	B	C	D	E
0	∞	∞	∞	∞
0	∞	2	∞	∞
0	4	2	∞	∞
0	∞	2	7	∞
0	4	∞	7	∞

Step 4 :- second iteration gurantees to give all the shortest path which are most 2 edges.

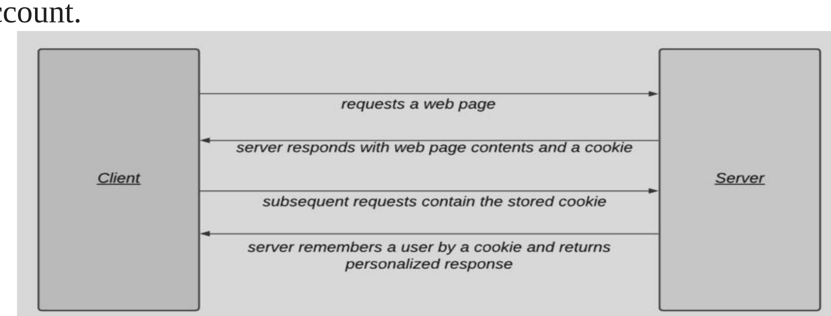
A	B	C	D	E
0	∞	∞	∞	∞
0	∞	2	∞	∞
0	4	2	∞	∞
0	∞	2	7	∞
0	4	∞	7	∞
0	10	2	7	∞
0	10	2	7	13
0	4	2	7	6

4.		**Attempt any <u>THREE</u> of the following:**	**12**
	a)	**Construct a diagram to show the application of cookies in a scenario in which the server uses Cookies for advertisement.**	**4M**
	Ans	Cookies are small files which are stored on a user's computer. They are used to hold a modest amount of data specific to a particular client and website and can be accessed either by the web server or by the client computer 	***Diagram 1M*** ***Steps 3M***

When cookies were invented, they were basically little documents containing information about you and your preferences. For instance, when you select your language in which you want to view your website, the website would save the information in a document called a cookie on your computer, and the next time when you visit the website, it would be able to read a cookie saved earlier.

That way the website could remember your language and let you view the website in your preferred language without having to select the language again.

A cookie can contain any type of information such as the time when you visited the website, the items that you added into your shopping basket, all the links you clicked in website, etc. Cookies themselves contain no personally identifiable information. Depending on the publisher's and the user's settings, information associated with cookies used in advertising may be added to the user's Google Account.

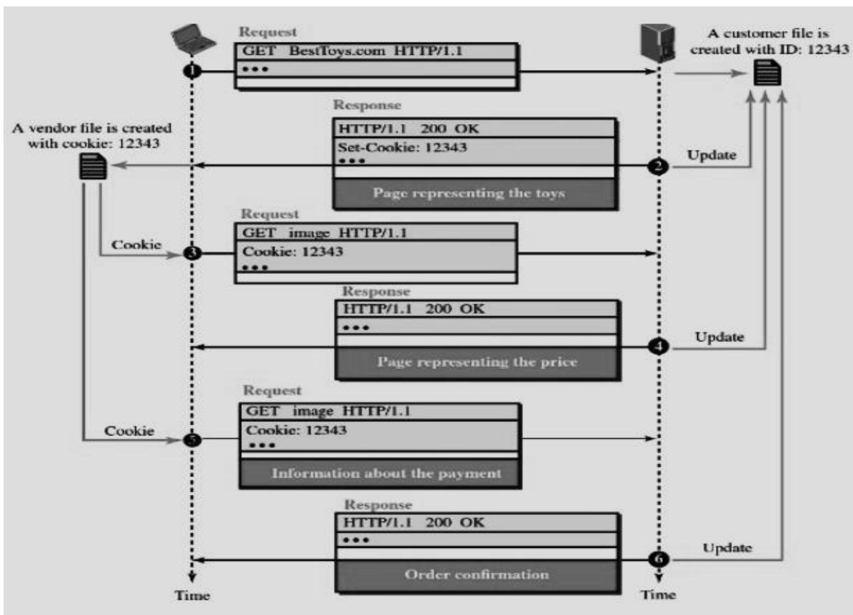


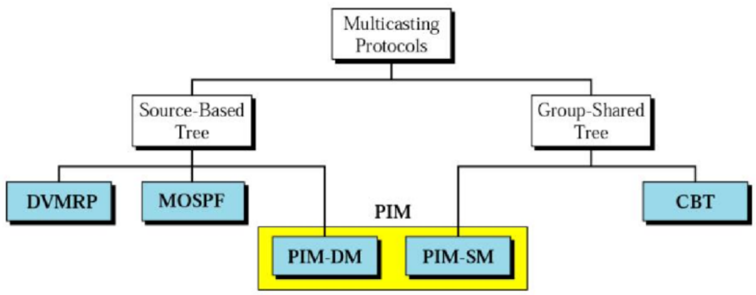
Most commonly, AdSense sends a cookie to the browser when a user visits a page that shows Google ads. Pages with Google ads include ad tags that instruct browsers to request ad content from our servers. When the server delivers the ad content, it also sends a cookie. But a page doesn't have to show Google ads for this to happen; it just needs to include our ad tags, which might load a click tracker or impression pixel instead.

Any Relevant answer shall be considered

		Following Fig. Example of how server uses cookies for advertisement.	

Subject: Advanced Computer Network (Elect) **Subject Code: 22520**



	b) **Ans.**	**List Intradomain multicast protocol. Explain any one in detail.** Intra domain routing protocols carry out the multi cast function within domains.  There are following three protocols play major roles in establishment multicast connections. 1) Multicast Distance Vector(DVMRP) 2) Multicast Link State(MOSPF) 3) Protocol Independent Multicast (PIM)	**4M** ***Diagram 1M*** ***List 1M*** ***Any one explanation 2M***

1) Multicast Distance Vector (DVMRP):

Distance vector routing when extended to support multicast is called Distance Vector Multicast Routing Protocol (DVMRP).

The DVMRP is Multicast routing protocol that takes the routing decision based upon the source address of the packet. This algorithm constructs the routing tree for a network.

Whenever, a router receives a packet, it forwards it to some of its ports based on the source address of the packet. The rest of the routing tree is made by downstream routers. In this way, routing tree is created from destination to source.

The DVMRP protocol must achieve the following tasks:

1. It must prevent the formation of loops in the network.
2. It must prevent the formation of duplicate packets.
3. It must ensure that the path travelled by a packet is the shortest from its source to the router.
4. It should provide dynamic membership.

It is a following two-stage process:

1. Create a broadcast mechanism that allows a packet to be forwarded to all the networks on the internet.
2. Refine this mechanism so that it prunes back networks that do not have hosts that belong to the multicast group.

Multicast distance vector routing uses source-based trees, but the router never actually makes a routing table. When a router receives a multicast packet, it forwards the packet as though it is consulting a routing table.

We can say that the shortest path tree is evanescent. After its use (after a packet is forwarded) the table is destroyed. To accomplish this, the multicast distance vector algorithm uses a process based on following four decision-making strategies:

1. Flooding:

It is the first strategy that comes to mind. A router receives a packet and without even looking at the destination group address, sends it out from every interface except the one from which it was received.

		Flooding accomplishes the first goal of multicasting: every network with active members receives the packet. However, so will networks without active members. This is a broadcast, not a multicast. There is another problem is, it creates loops. A packet that has left the router may come back again from another interface or the same	

SUMMER – 2023 EXAMINATION

MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code: 22520**

interface and be forwarded again.

Some flooding protocols keep a copy of the packet for a while and discard any duplicates to avoid loops. The next strategy, reverse path forwarding, corrects this defect.

2. Reverse Path Forwarding (RPF):

RPF is a modified flooding strategy. RPF eliminates the loop in the flooding processes.

In this strategy, the router only forwards those packets that have travelled the shortest path from source to destination.

To achieve this, the router pretends that it has a packet to send to the source from has arrived. In this way, the shortest path to the sender of the packet is computed.

If the same route is followed by the received packet, it is forwarded to the next router and it is discarded otherwise.

The reverse path forwarding ensures that the network receives a copy of the packet without formation of loops. A loop occurs when a packet that has left the router may come back again from another interface or the same interface and be forwarded again.

RPF does not guarantee that there would be no duplicate packets in the network i.e. the network may receive two or more copies. The reason for this is that the routing is based on the source address and not on the destination address.

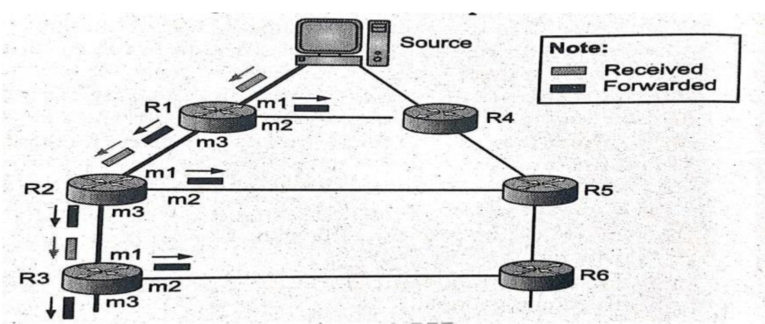


Fig. RPF

3. Reverse Path Broadcasting (RPB)

		RPF does not guarantee that each network receives only one copy a network receives two or more copies. The reason is that RPF is not based on the destination address forwarding is based on the source address. In order to solve the problem, RPB is used.	

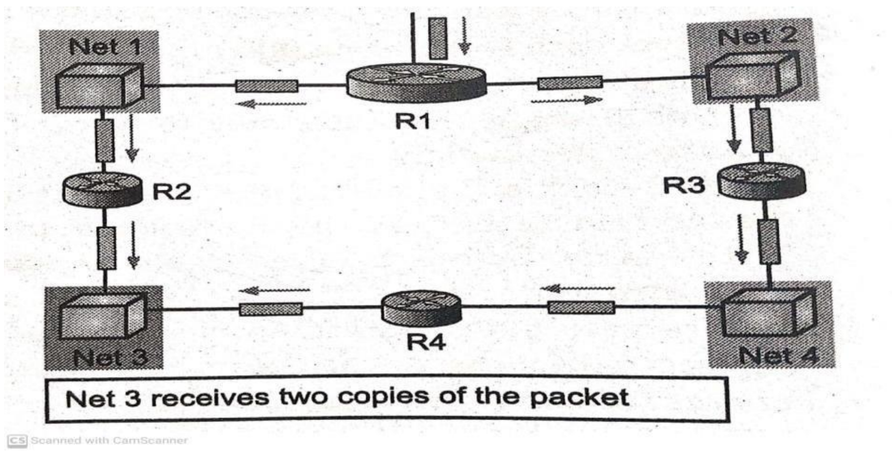


Fig. Problem with RPF

Consider the above Fig in which Net3 receives two copies of the packet even though each router just sends out one copy from each interface. There is duplication because a tree has not been made instead of a tree we have a graph. Net3 has two parents namely, routers R2 and R4.

In RPB method, one parent router is defined for each network. The network could accept the multicast packets from this parent router only. This router sends packets to those ports for which it is designated as parent.

Thus, RPB principle allows a router to broadcast the packet in the network. This creates duplicate packets on the network and reduces the network efficiency

To eliminate duplication, we must define only one parent router for each network. We must have this restriction: A network can receive a multicast packet from a particular source only through a designated parent router.

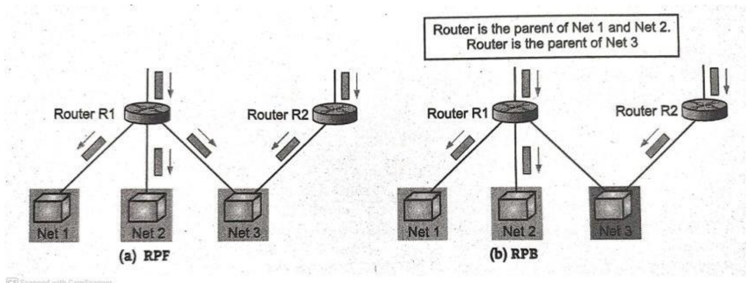
Now the policy is clear. For each source, the router sends the packet only out of those interfaces for which it is the designated parent. This policy is called Reverse Path Broadcasting (RPB).

		RPB guarantees that the packet reaches every network and that every network receives only one copy. Following Fig, shows the difference between RPF & RPB	

SUMMER – 2023 EXAMINATION

MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code: 22520**



4. Reverse Path Multicasting (RPM):

To overcome the problem of broadcasting in RPB, Reverse Path Multicasting in used. In RPM the desired multicast network tree is created by using two methods namely, Pruning and Grafting. A router can send a prune message to its upstream router whenever it finds that its network is not interested in a multicast packet. In this way a router prunes (cuts) its network from multicasting.

If a router receives prune message from all the downstream routers, it in turn, sends a prune Message to its upstream router.

To convert broadcasting to multicasting, the protocol uses following two procedures, pruning and grafting. **i) Pruning:**

The designated parent router of each network is responsible for holding the membership information. This is done through the IGMP protocol.

The process starts when a router connected to a network finds that there is no interest in a multicast packet. The router sends a prune message to the upstream router so that it can prune the corresponding interface.

That is, the upstream router can stop sending multicast messages for this group through that interface. Now if this router receives prune messages from all downstream routers, it, in turn, sends a prune message to its upstream router.

(ii) Grafting:

		What if a leaf router (a router at the bottom of the tree) has sent a prune message but suddenly realizes, through IGMP, that one of its networks is again interested in receiving the multicast packet? It can send a graft message. The graft message forces the upstream router to resume sending the multicast messages.	

Following Fig. shows the idea of pruning and grafting.

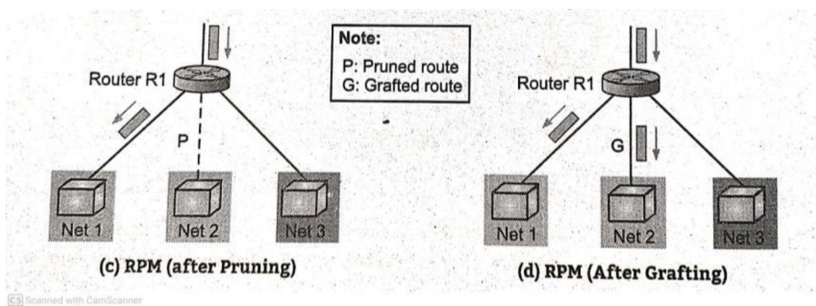


Fig.RPM Pruning and Grafting

2) Multicast Link State (MOSPF)

MOSPF protocol is an extension of the OSPF protocol that uses multicast link state routing to create source based trees.

MOSPF provides enhancements to OSPF Version 2 (OSPFV2) to support IP multicast routing.

The protocol requires a new link state update packet to associate the unicast address of a host with the group address only report directly connected hosts. This packet is called the group-membership LSA (Link State Advertisement).

MOSPF is a data driven protocol; the first time an MOSPF router sees a datagram with a given source and group address, the router constructs the Dijkstra shortest path tree.

MOSPF takes advantage of the link-state information maintained by OSPF.

Using the link-state and group membership information, MOSPF routers are able to calculate pruned source rooted shortest-path trees for multicast datagrams by using the Dijkstra's algorithm.

MOSPF also defines a mechanism for inter-AS multicast forwarding.

The biggest disadvantage of MOSPF is that every router must maintain membership information of every group. Therefore, MOSPF also scales poorly if there are many multicast groups.

When compared to DVMRP, MOSPF causes no useless data traffic.

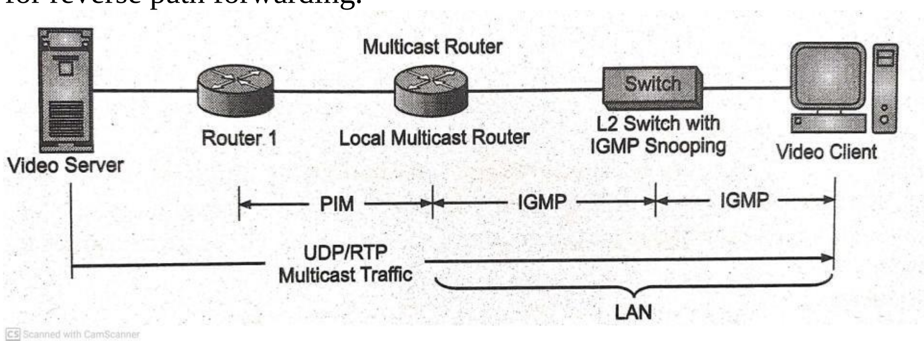
		3) Protocol Independent Multicast (PIM) PIM emerged as an algorithm to overcome the limitations of protocol such as the Distance Vector Multicast Routing Protocol (DVMRP),	

PIM was designed to avoid the dense-mode scaling issues of DVMRP and the potential performance issues of CBT (Core Base Tree) at the same time.

PIM is used for efficient routing to multicast groups that might span wide-area and inter domain internetworks. It is called “protocol independent” because it does not depend on a particular unicast routing protocol.

Protocol Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-tomany and many-to-many distribution of data over a LAN, WAN or the Internet.

PIM is not dependent on a specific unicast routing protocol; it can make use of any unicast routing protocol in use on the network. PIM does not build its own routing tables. PIM uses the unicast routing table for reverse path forwarding.



Protocol Independent Multicast (PIM) is the name given to two independent multicast routing protocols namely, Protocol Independent Multicast, Dense Mode (PIM-DM) and Protocol Independent Multicast, Sparse Mode (PIM-SM). Both protocols are unicast-protocol dependent, but the similarity ends here.

		) **PIM-DM:** PIM Dense Mode (PIM-DM) is a multicast routing protocol designed with the opposite assumption to PIM-SM, namely that the receivers for any multicast group are distributed densely throughout the network. PIM-DM is used when there is a possibility that each router is involved in multicasting (dense mode). In this environment, the use of a protocol that broadcasts the packet is justified because almost all routers are involved in the process.	

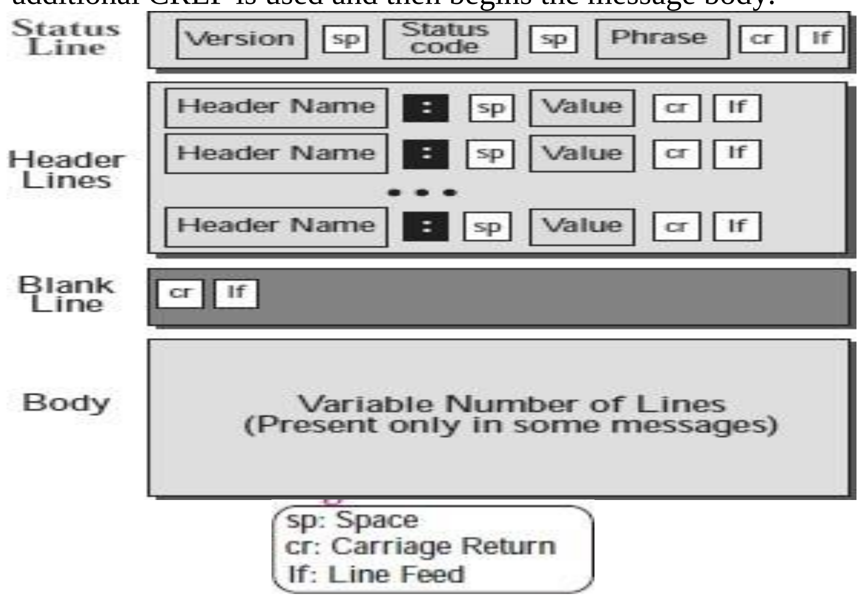
		PIM-DM is a source-based tree routing protocol that uses RPF and pruning/grafting strategies for multicasting. Its operation is like DVMRP; however, unlike DVMRP, it does not depend on a specific unicasting protocol. It assumes that the autonomous system is using a unicast protocol and each router has a table that can find the outgoing interface that has an optimal path to a destination. This unicast protocol can be a distance vector protocol (RIP) or link state protocol (OSPF). PIM-DM is used in a dense multicast environment, such as a LAN. PIM-DM uses RPF and pruning/grafting strategies to handle multicasting. However, it is independent from the underlying unicast protocol.	

		) **PIM-SM:** PIM Sparse Mode (PIM-SM) is a multicast routing protocol designed on the assumption that recipients for any particular multicast group will be sparsely distributed throughout the network. PIM-SM is used when there is a slight possibility that each router is involved in multicasting (sparse mode). In this environment, the use of a protocol that broadcasts the packet is not justified; a protocol such as CBT (Core Base Tree) that uses a group-shared tree is more appropriate. PIM-SM is a group-shared tree routing protocol that has a Rendezvous Point (RP) as the source of the tree. Its operation is like CBT; however, it is simpler because it does not require acknowledgment from a join message. PIM-SM is used in a sparse multicast environment such as a WAN. PIM-SM is similar to CBT but uses a simpler procedure.	
	c) **Ans.**	**Describe the HTTP Responses Message Format.** A Response message consists of a status line header line, a blank line and sometimes a body. HTTP Response sent by a server to the client. The response is used to provide the client with the resource it requested. It is also used to inform the client that the action requested has been carried out. It can also inform the client that an error occurred in processing its request.	**4M** ***Diagram 1M*** ***Explanation 3M***

An HTTP response contains the following things:

1. Status Line
2. Response Header Fields or a series of HTTP headers
3. Blank Line
4. Message Body

In the request message, each HTTP header is followed by a carriage returns line feed (CRLF). After the last of the HTTP headers, an additional CRLF is used and then begins the message body.



1) Status Line :

In the response message, the status line is the first line. The status line contains three items:

a) HTTP Version Number: It is used to show the HTTP specification to which the server has tried to make the message comply.

b) Status Code: It is a three-digit number that indicates the result of the request. The first digit defines the class of the response. The last two digits do not have any categorization role. There are five values for the first digit, which are as follows:

Any relevant explanation shall be considered.

		Code and Description: **1xx:** Information It shows that the request was received and continuing the process. **2xx:** Success It shows that the action was received successfully, understood, and accepted. **3xx:** Redirection It shows that further action must be taken to complete the request. **4xx:** Client Error It shows that the request contains incorrect syntax, or it cannot be fulfilled. **5xx:** Server Error It shows that the server failed to fulfil a valid request. **c) Reason Phrase:** It is also known as the status text. It is a humanreadable text that summarizes the meaning of the status code. **2) Header Lines :** The HTTP Headers for the response of the server contain the information that a client can use to find out more about the response, and about the server that sent it. This information is used to assist the client with displaying the response to a user, with storing the response for the use of future, and with making further requests to the server now or in the future. The name of the Response-header field can be extended reliably only in combination with a change in the version of the protocol. **3) Blank Line :** It contains cr (Carriage Return) & if (Line Feed) **4)** **Entire Body:** The body of the message is used for most responses. The exceptions are where a server is using certain status codes and where the server is responding to a client request, which asks for the headers but not the response body.	

d) **List different timers used in TCP.** **4M**

Ans. TCP uses several timers to ensure that excessive delays are not encountered during communications.

Several of these timers are elegant, handling problems that are not immediately obvious at first analysis. Each of the timers used by TCP is examined in the following subsections, which reveal its role in ensuring data is properly sent from one connection to another. TCP implementations use at least four timers as shown in following Fig.

Diagram 1M

List 1M

Explanation 2M

Any other relevant explanation shall be considered.

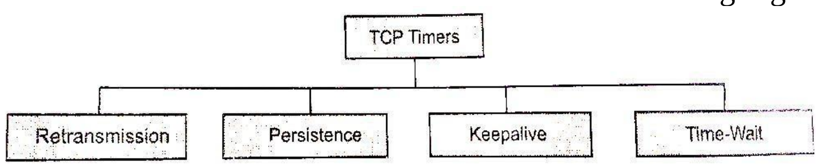


Fig.TCP Timers 1) Retransmission Timer:

To retransmit lost segments, TCP uses Retransmission Time Out (RTO). When TCP sends a segment the timer starts and stops when the acknowledgment is received.

If the timer expires timeout occurs and the segment is retransmitted.

RTO (retransmission timeout is for 1 RTT) to calculate retransmission timeout we first need to calculate the RTT.

Three Types of RTT:

1. Measured RTT (RTTm): The measured Round Trip Time (RTT) for a segment is the time required for the segment to reach the destination and be acknowledged, although the acknowledgment may include other segments.

2. Smoothed RTT (RTTS): It is the weighted average of RTTm. RTTM is likely to change and its fluctuation is so high that a single measurement cannot be used to calculate RTO.

(i)	Initially	No value
(ii)	After the first measurement	RTTs=RTTm.
(iii)	After each measurement	RTTs-(1-1)*RTTs+t*RTTm.

SUMMER – 2023 EXAMINATION

MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code: 22520**

3. Deviated RTT (RTTd): Most implementation do not use RTTS alone so RTT deviated is also calculated to find out RTO.

(i)	Initially	No value
(ii)	After first measurement	RTTd=RTTm/2
(iii)	After each measurement	RTTd=(1-k)*RTTd+k* (RTTm - RTTS)

Retransmission Timeout:

RTO Calculation: The value of RTO is based on the smoothed round-trip time and its deviation. Most implementations use the following formula to calculate the RTO:

Initial value → Original (given in question).

After any measurement→RTO=RTTs +4*RTTd

2) Persistent Timer:

To deal with a zero-window-size deadlock situation, TCP uses a persistence timer. When the sending TCP receives an acknowledgment with a window size of zero, it starts a persistence timer.

When the persistence timer goes off, the sending TCP sends a special segment called a probe. This segment contains only 1 byte of new data. It has a sequence number, but its sequence number is never acknowledged; it is even ignored inCalculating the sequence number for the rest of the data. The probe causes the receiving TCP to resend the acknowledgment which was lost.

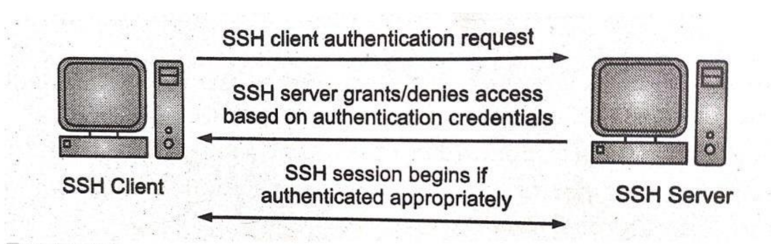
3) Keepalive Timer:

A keepalive timer is used to prevent a long idle connection between two TCPs. If a client opens a TCP connection to a server transfers some data and becomes silent the client will crash.

In this case, the connection remains open forever. So a keepalive timer is used. Each time the server hears from a client, it resets this timer. The time-out is usually 2 hours. . If the server does not hear from the client after 2 hours, it sends a probe segment. If there is no response after 10 probes, each of which is 75 s apart, it assumes that the client is down and terminates the connection.

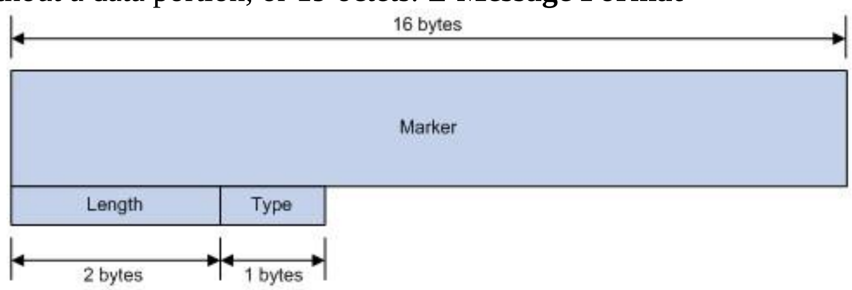
		4) Time Wait Timer: This timer is used during TCP connection termination. The timer starts after sending the last Ack for 2nd FIN and closing the	

		connection. After a TCP connection is closed, it is possible for datagrams that are still making their way through the network to attempt to access the closed port. The quiet timer is intended to prevent the just closed port from reopening again quickly and receiving these last datagrams. The quiet timer is usually set to twice the maximum segment lifetime (the same value as the Time- To-Live field in an IP header), ensuring that all segments still heading for the port have been discarded.	

	e) Ans.	**Explain the working of SSH.** SSH (Secure Shell) is the most popular remote login application program. SSH uses client-server architecture in its implementation. An SSH server can be deployed and allow several SSH clients to connect to it. The architecture of SSH is shown in following Fig. and the SSH process is as follows: 1) The SSH client on the left provides authentication to the SSH server on the right. In the initial connection, the client receives a host key of the server, therefore, in all subsequent connections, the client will know it is connecting to the same SSH server. This places less emphasis on the IP address of the SSH server, which can be easily spoofed, and more emphasis on the host key of the server, which cannot be spoofed very easily. 2) The SSH server determines if the client is authorized to connect to the SSH service by verifying the username/password or public key that the client has presented for authentication. This process is completely encrypted. 3) If the SSH server authenticates the client and the client is authorized, the SSH session begins between the two entities. All communication is completely encrypted.  **Fig. SSH Communication from an SSH Client to an SSH Server**	**4M** *Diagram 1M* *Explanation 3M* *Any relevant explanation may be considered*

		The steps involved in creating an SSH session go like this: 1. Client contacts server to initiate a connection. 2. The server responds by sending the client a public cryptography key. 3. The server negotiates parameters and opens a secure channel for the client. 4. The user, through their client, logs into the server.	

5.		**Attempt any TWO of the following:**	**12**
	a)	**Describe the BGP3 in detail.**	**6M**
	Ans.	• To denote any protocol used to pass routing information between two autonomous systems, Computer scientists use the term Exterior Gateway Protocol (EGP). Currently a single exterior protocol is used in most TCPJIP internets. Known as the Border Gateway Protocol (BGP), it has evolved through four (quite different) versions one of the versions is BGP3. • Two systems form a transport protocol connection between one another. They exchange messages to **open** and confirm the connection parameters. The initial data flow is the entire BGP routing table. • Incremental **updates** are sent as the routing tables change. BGP does not require periodic refresh of the entire BGP routing table. Therefore, a BGP speaker must retain the current version of the entire BGP routing tables of all of its peers for the duration of the connection. • **Keepalive** messages are sent periodically to ensure the liveness of the connection. • Notification messages are sent in response to errors or special conditions. If a connection encounters an error condition, a **notification** message is sent and the connection is closed. • Connections between BGP speakers of different ASs are referred to as "external" links. BGP connections between BGP speakers within the same AS are referred to as "internal" links. • Messages are sent over a reliable transport protocol connection. A message is processed only after it is entirely received. The maximum message size is 4096 octets. All implementations are required to support this maximum message size.	***Explanation 3M for Message Format diagram and explanation with message types 3M***

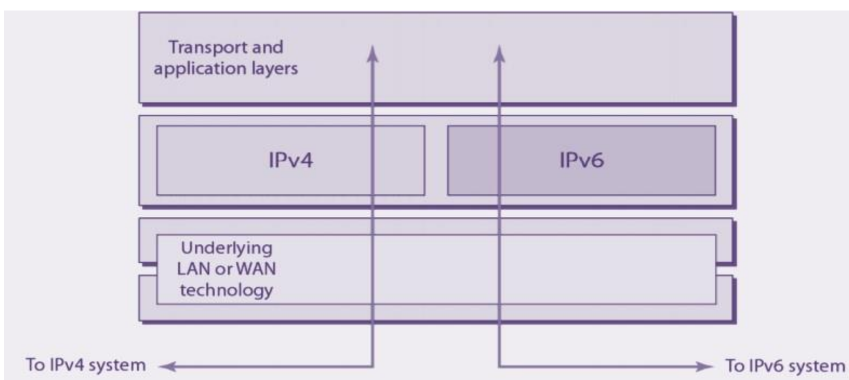
		• The smallest message that may be sent consists of a BGP header without a data portion, or 19 octets. **Message Format**  • **Marker** If the Type of the message is OPEN, or if the Authentication Code used in the OPEN message of the connection is zero, then the Marker must be all ones. The Marker can be used to detect loss of synchronization between a pair of BGP peers, and to authenticate incoming BGP messages. • **Length** This 2-bytes unsigned integer indicates the total length of the message, including the header, in bytes. • **Type** This 1-byte unsigned integer indicates the type code of the message. The following type codes are defined: 1 - OPEN 2 - UPDATE 3 - NOTIFICATION 4 – KEEPALIVE • **OPEN Message** After a transport protocol connection is established, the first message sent by each side is an OPEN message. If the OPEN message is acceptable, a KEEPALIVE message confirming the OPEN is sent back. Once the OPEN is confirmed, UPDATE, KEEPALIVE, and NOTIFICATION messages may be exchanged. • **UPDATE Message**	

		UPDATE messages are used to transfer routing information between BGP peers. The information in the UPDATE packet can be used to construct a graph describing the relationships of the various Autonomous Systems.	

		NOTIFICATION Message A NOTIFICATION message is sent when an error condition is detected. The BGP connection is closed immediately after sending it. **KEEPALIVE Message** BGP does not use any transport protocol-based keep-alive mechanism to determine if peers are reachable. Instead, KEEPALIVE messages are exchanged between peers often enough.	

	b)	**State the need for** **1. Sequence Control** **2. Error Control** **3. Flow Control in Networking**	**6M**
	Ans.	**Sequence Control** The 32-bit sequence number field defines the number assigned to the first byte of data contained in this segment. TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence comprises the first byte in the segment. During connection establishment, each party uses a Random number generator to create an initial sequence number (ISN), which is usually different in each direction. We know that a TCP sequence number is 32 bit. So it has finite (from 0 to (232-1) = 4 Giga sequence numbers) and it means we will be able to send only 4GB of data with a unique sequence number not more than that. It helps with the allocation of a sequence number that does not conflict with other data bytes transmitted over a TCP connection. An ISN is unique to each connection and separated by each device. **Error Control** Error Control mechanisms are useful to ensure reliability service of TCP. To provide reliable service TCP detects and corrects errors. Error control mechanisms are useful for detecting corrupted segments, lost segments, out-of-order segments, and duplicated segments. Error detection and correction in TCP is achieved through the use of three simple tools: checksum, acknowledgment, and time-out.	***2M for each***

		Flow Control Flow control make it possible for sender to send the amount of data bytes that can be sent without worrying an acknowledgment and is one of the most important duties of the data link layer. In most protocols, flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow Control procedures not allowed to overwhelm the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data, if sender sends data in a much speed data loss may occur to overcome this problem flow control procedures are needful.	

	c)	**Explain the process of transition from of IPv4 to IPv6 for a network.**	6M
	Ans.	Three Transition from IPv4 to IPv6 strategies are 1. Dual Stack 2. Tunnelling 3. Header Translation **1. Dual Stack** In this kind of strategy, a station has a dual stack of protocols run IPv4 and IPv6 simultaneously. To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.  Fig. Dual Stack	*2M for each transition*

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

SUMMER – 2023 EXAMINATION

MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code: 22520**

2. Tunnelling

Tunnelling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4.

- To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region.
- To make it clear that the IPv4 packet is carrying an IPv6 packet as data.

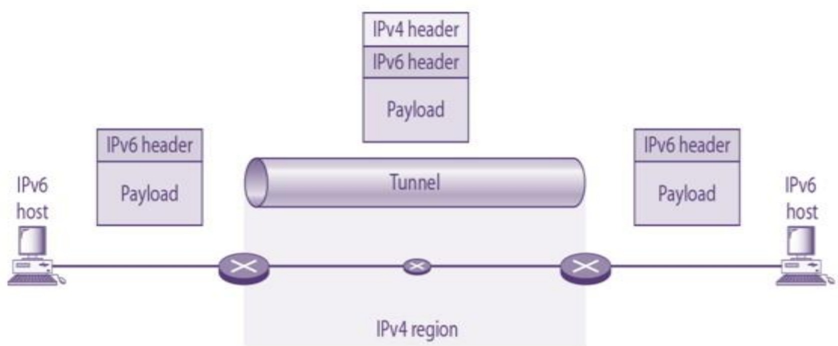


Fig. Tunnelling

3. Header Translation

In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header see figure.

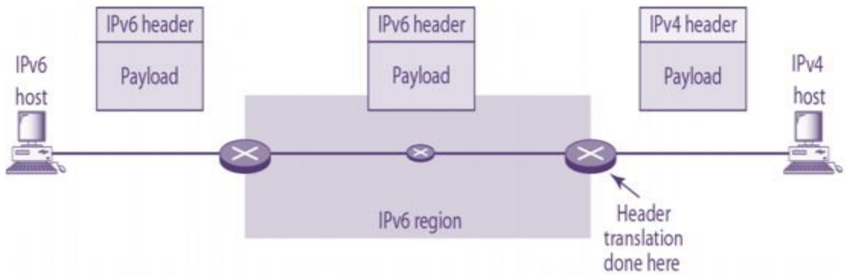


Fig. Header Translation

6.		**Attempt any TWO of the following:**	**12**

a) **With a suitable example, explain Link State Routing algorithm. What are the serious drawbacks of Link State Routing Algorithm?**
(Any relevant explanation can be considered) — **6M**

Ans.

4M for explanation with example

2M for drawbacks

In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.

1. Creation of the states of the links by each node, called the link state packet(LSP).
2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.
3. Formation of a shortest path tree for each node. (Dijkstra algorithm)
4. Calculation of a routing table based on the shortest path tree.

Example*(Any relevant example explained can be considered)*
Consider a sample network of networks. There are seven networks numbered 1 to 7, connected to each other by six routers A through F. As we will notice, each router is connected to at least two networks, but it may also be connected to more than two networks, e.g., router A in the figure.
Assume the following are cost values

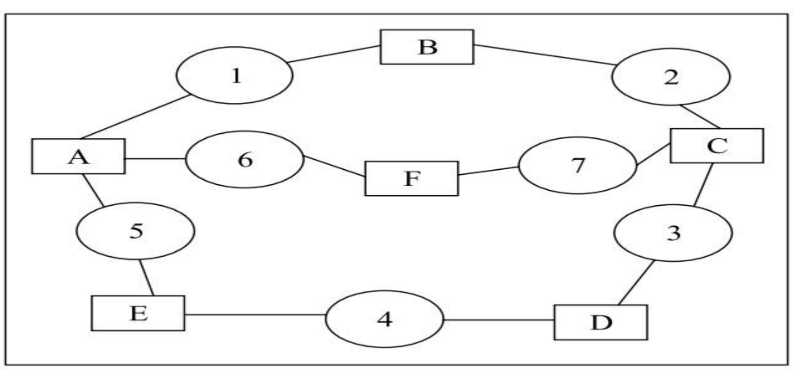


Fig. A

graph for Internet (Where nodes denotes routers)

Periodically, each router sends a very small greeting packet to each of its neighbors and expects a response back from the neighbor. If the

		neighbor reverts, the original router considers that the neighbor is up and running, and accordingly determines the cost based on the factors discussed earlier. Otherwise, the neighbor is considered to be in some error. Using this information, the original router then sends information	

SUMMER _ 2023 EXAMINATION

MODEL ANSWER

Subject: Advanced Computer Network (Elect) **Subject Code: 22520**

about all its neighbors to the entire Internet in a process called flooding, as discussed earlier. For this, it sends a special packet called Link State Packet (LSP) to all other routers via its neighbors.

For example, a sample portion of the LSP (shown only for router A about its neighbors) could take the form as shown below

LSP for r

Advertiser	Network	Cost	Neighbor
A	1	1	B
A	6	3	F
A	5	2	E

outer A (Cost is Assumed in example)

For example, the first row says that between router A (the first column) and router B (the fourth column), there is network 1 (the second column), and that the cost of going from router A to router B is 1 (the fourth column).

Every router receives every LSP packet, and uses it to create a local database called link state database. Thus, a link state database is a collection of all LSPs. Every router stores such a database on its disk, and uses it for routing packets. A sample link state database for our example Internet is shown below

Advertiser	Network	Cost	Neighbor
A	1	1	B
A	6	3	F
A	5	2	E
B	1	4	A
B	2	2	C
C	2	5	B
C	3	2	D
D	3	5	C
D	4	3	E
E	5	3	A
E	4	2	D
F	6	2	A
F	7	3	–

Link State Database

Having constructed the link state database, each router executes an

		algorithm called Dijkstra algorithm to create its routing table. This algorithm considers the Internet as a graph, and finds the distance along a shortest path from a single node of the graph to all other nodes in the graph. Using this information, a routing table is created to compute the shortest path. This algorithm must be run for each routing table once. **Drawbacks** • **Memory Requirements** − the link-state routing algorithm creates and maintains a database and SPF tree. The database and SPF tree required more memory than a distance vector algorithm. • **Processing Requirements** − to build a complete map of the topology Link-state routing protocols also require more CPU processing. • **Bandwidth Requirements** − The link-state routing protocol floods link-state packet during initial start-up and also at the event like network breakdown, and network topology changes, which affect the available bandwidth on a network. If the network is not stable it also creates issues on the bandwidth of the network. 	

	b)	**For the IP addresses given below** **1. Identify the classes to which the following IP address belongs to** **2. Identify network address sections** **3. Identify host address section** **4. Calculate number of hosts that can be assigned with each network** **i. 22.34.45.133 ii.** **12.12.12.12 iii.** **192.0.233.26 iv.** **126.123.16.87**	**6M**
	Ans.	**22.34.45.133**= 00010110.00100010.00101101.10000101 IP address class = Class A Network Section = 00010110 = 22 Host Section = 00100010.00101101.10000101= 34.45.133 Number of Host/Network = 2^{24}-2 = 16,777,214 **12.12.12.12**= 00001100.00001100.00001100.00001100 IP address class = Class A Network Section = 00001100 = 12	***Each IP address*** $1\frac{1}{2}$ ***description M***

		Host Section = 00001100.00001100.00001100= 12.12.12 Number of Host/Network = 2^{24}-2 = 16,777,214 **192.0.233.26**= 11000000.00000000.11101001.00011010 IP address class = Class C Network Section = 11000000.00000000.11101001 = 192.0.233 Host Section = 00011010= 26 Number of Host = 2^8-2 = 154 **126.123.16.87**= 01111110.01111011.00010000.01010111 IP address class = Class A Network Section = 01111110 = 126 Host Section = 01111011.00010000.01010111= 123.16.87 Number of Host = 2^{24}-2 = 16,777,214	

	c) Ans.	**Describe e-mail security over non-secure channel.** ***(Note: Any other description of the concept shall be considered.)*** • Email security describes different techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss or compromise. • Email is often used to spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to part with sensitive information, open attachments or click on hyperlinks that install malware on the victim's device. • Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than intended recipients. Email encryption often includes authentication. • Email allows attackers to use it as a way to cause problems in attempt to profit. Whether through spam campaigns, malware and phishing attacks, sophisticated targeted attacks, or business email compromise (BEC), attackers try to take advantage of the lack of security of email to carry out their actions. • Since most organizations rely on email to do business, attackers exploit email in an attempt to steal sensitive information. • Because email is an open format, it can be viewed by anyone who can intercept it. It can be easily read and the contents of an email by intercepting it. • Email Security Policies can be established by viewing the contents of emails flowing through their email servers. It's important to	**6M** ***Any six points 1M each***

		understand what is in the entire email in order to act appropriately. After these baseline policies are put into effect, an organization can enact various security policies on those emails. • These email security policies can be as simple as removing all executable content from emails to more in-depth actions, like sending suspicious content to a sandboxing tool for detailed analysis. • If security incidents are detected by these policies, the organization needs to have actionable intelligence about the scope of the attack. • Enforce email encryption policies to prevent sensitive email information from falling into the wrong hands. • An email gateway scans and processes all incoming and outgoing email and makes sure that threats are not allowed in. Because attacks are increasingly sophisticated, standard security measures, such as blocking known bad file attachments, are no longer effective.	